Deloitte. | Google Cloud

AGENTIC COMMERCE READINESS

FOR RETAIL AND CONSUMER PRODUCTS ORGANIZATIONS

Executive summary

Agentic commerce is moving from an emerging concept to an operational reality for some retail and consumer products (RCP) organizations. Today, 55% of consumers report using Generative AI (GenAI) to begin shopping journeys[1] – and as large language model (LLM) platforms become more accessible and trusted, AI agents will increasingly drive discovery, evaluation, and transactions: often outside brand-owned digital properties. The competitive divide will likely not be defined by who experiments with agents first, but by which organizations are structurally prepared to drive agent-led commerce execution at scale.

Agentic commerce readiness is not limited to integrating enterprise systems with LLMs or conversational interfaces. It requires deliberate preparation across data, technology, infrastructure, trust, and operating models so that enterprise systems can respond reliably, securely, and efficiently when agents act on behalf of customers, brands, or partners. As agentic interactions increasingly occur off brand owned properties and within third party agent ecosystems, agentic commerce should be treated as a distinct channel with unique execution requirements, risk characteristics, and performance metrics. Organizations can participate in agentic commerce in three primary ways:

1. Agentic platform experiences (such as, AI-powered discovery and decisioning within Google AI Mode or the Gemini app)
2. Agentic experiences on owned retailer surfaces (such as, shopping assistants)
3. Agent-to-agent interactions, where consumer agents interact with retailer and brand agents through shared protocols

While these models differ in ownership and orchestration, all require the same foundational readiness, with minor variations in implementation, controls and governance. This paper outlines what agentic commerce readiness means for retail and consumer product organizations, and describes the progressive capability shifts organizations should anticipate.

AGENTIC COMMERCE AND THE SHIFT IN EXECUTION

Traditional digital commerce architectures were built for supporting human-driven journeys, assuming people would browse, compare and transact step by step. Agentic commerce changes this model by compressing discovery, evaluation and transaction into a single delegated action, often executed outside the brand-owned experience. As purchases shift from screens designed for customers to machine-to-machine interactions, organizations must provide fast, reliable, and machine-readable access to product data, pricing, offers, availability, policies, and fulfillment.

This shift creates a fundamental inversion of trust. In traditional commerce, consumers place trust in brands through familiarity, reputation, and experience. In agentic commerce, trust migrates to the integrity of protocols and the agent itself: a consumer does not need to independently evaluate a thousand merchants if they trust the agent acting on their behalf. For organizations, this means credibility is increasingly expressed through technical standards, verifiable agent identity (Know Your Agent), secure payment protocols, and machine-readable policy transparency, rather than through brand messaging alone.

Organizations unprepared for this shift could lose influence and relevance as agents increase their commerce market share and drive growth by using dynamic offers that are easier to evaluate, verify, and execute. Once offers are located, conversion is increasingly influenced by real-time incentives: some players such as Google have developed 'Direct Offer' engines that trigger dynamic promotions such as limited-time loyalty bonuses, price incentives or expedited fulfillment to increase the likelihood of conversion times and rates.[2]

Figure 1: Customer touchpoints in traditional e-commerce vs. agentic commerce

DEFINING AGENTIC COMMERCE READINESS

Agentic commerce readiness should be understood as a progressive capability shift rather than a binary state. Organizations typically evolve through three broad stages as they adapt to agent-led execution: agent aware, agent compatible, and agent native. These stages reflect increasing levels of structural alignment between enterprise systems and the needs of autonomous agents.

AGENT NASCENT

Agent nascent organizations have not yet meaningfully engaged with agentic commerce and, in some cases, actively block or constrain agent access through existing digital controls. Agent interactions are largely invisible, data and systems are designed exclusively for human use, and there is no clear strategy or ownership for agent-led execution. Security, technology, and operating models are not prepared to distinguish or support trusted agents, leaving the organization unprepared to respond as agent activity increases. The primary risk at this stage is sudden disruption, as agents bypass the organization entirely in favor of more accessible alternatives.

AGENT AWARE

Agent aware organizations recognize that agents are already interacting with their digital ecosystem, with agent-originated traffic, inquiries, or transactions visible in analytics or logs – even though systems are not designed to support or shape these interactions. Product and policy information is often inconsistent or incomplete from a machine perspective, and while APIs may exist, they are typically built for internal or partner use rather than autonomous execution. Security and fraud controls typically treat agents as indistinguishable from bots, limiting the organization's ability to differentiate trusted delegated activity from malicious automation. This creates visibility but not control, exposing architectural misalignment, data quality constraints and a limited ability to respond operationally. The primary risk at this stage is silent erosion, as agents may route around the organization, substitute products, or favor competitors without triggering obvious failures.

AGENT COMPATIBLE

Agent compatible organizations take deliberate steps to enable agent-led interactions, with core commerce capabilities such as pricing, offers, availability, and fulfillment accessible programmatically in near real time. Product and policy data is structured, current, and sufficiently complete to support agent decision-making. Agentic commerce is treated as a distinct channel, with guardrails, early governance models and pilots for identity and delegated payment capabilities to enable limited autonomous transactions. While agent compatibility enables participation, it does not guarantee differentiation: leaving many organizations functionally accessible but largely interchangeable.

AGENT NATIVE

Agent native organizations design commerce capabilities with agent execution as a primary consideration, optimizing for low-latency, event-driven interaction and using data as a control plane for autonomous decisions governed by explicit contracts. Organizations may deploy their own retailer or brand agents to participate in agent-to-agent interactions, with trust, identity, and consent enforced at machine scale. Agentic commerce is supported by an operating model designed for adoption, with clear ownership, cross-functional workflows, change management, and incentives that embed agent-led execution into day-to-day operations. As a result, agentic commerce is managed like any other core channel, with defined metrics, investment decisions, and accountability.

Figure 2: Evolution of agentic commerce readiness

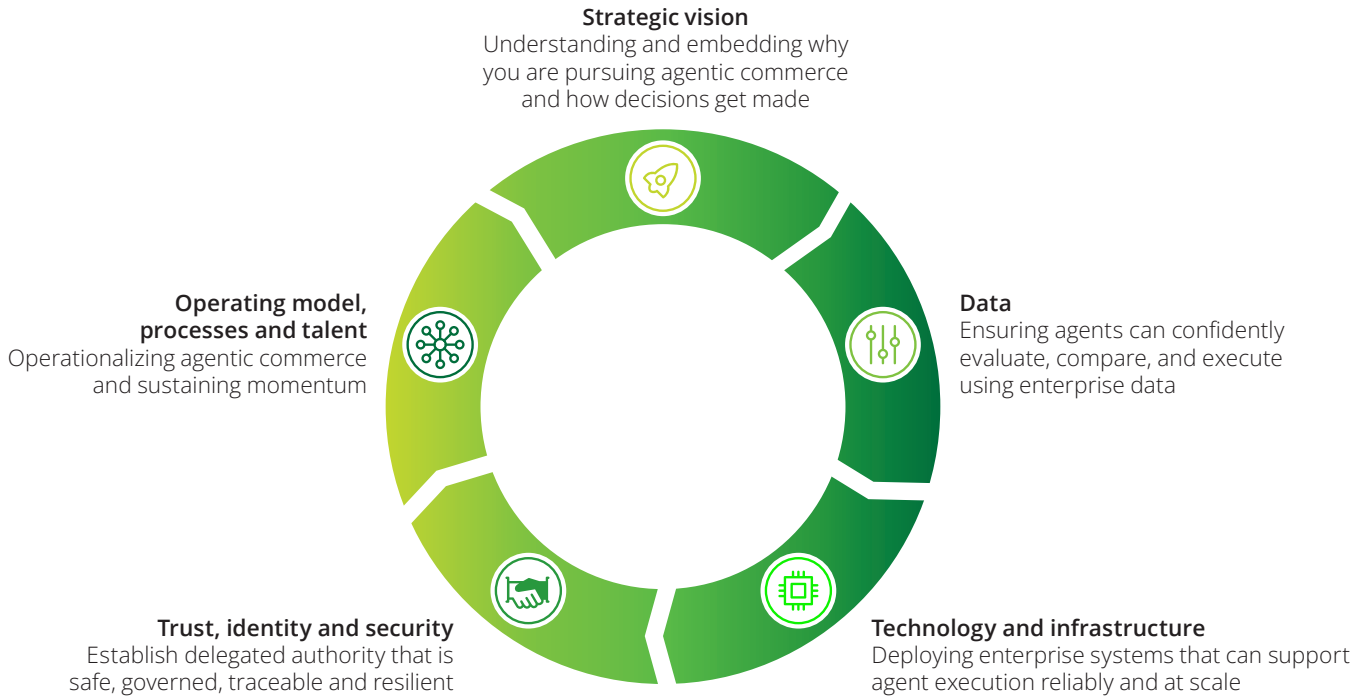
	Agent nascent	Agent aware	Agent compatible	Agent native
Strategic vision	**No defined** agent ambition or strategy	**Awareness** without organization or ownership	**Intentional** agent strategy	**Agent-led** strategy embedded within operations
Data	Human-oriented, **fragmented** data	**Machine-readable**, but unaudited, data	Structured, **agent-readable** data	Data as a **control plane**
Technology and infrastructure	Latency-prone **legacy** stack	**Systems exposed**, not designed	Agent-enabled **platform extensions**	**Purpose-built, event-driven** agent infrastructure
Trust, identity and security	Agents **blocked** or untrusted	Agents treated as **bots**	**Delegated** trust pilots	Contracted, **machine-scale** trust
Operating model, process, talent	**No ownership** or control	**Reactive** manual oversight	**Governed** agent execution	Agent operations **institutionalized**

CORE READINESS DIMENSIONS

Agentic commerce readiness requires synchronized maturity across all foundational dimensions, as agents interact with enterprises as integrated systems rather than isolated capabilities. Progress in data, technology, or infrastructure alone is insufficient if trust, security, operating models, or measurement lag behind. Where readiness is fragmented, agents introduce friction by design; bypassing organizations that cannot support reliable, trusted, end-to-end execution.

- **Strategic vision readiness:** Defining a clear agentic commerce ambition supported by executive sponsorship, established decision rights, and explicit business outcomes. Leading organizations move beyond experimentation to position agentic commerce as a strategic driver of growth, efficiency, and relevance, supported by new, agentic-specific KPI tracking and insight-to-action mechanisms that translate agent signals into informed decisions.
- **Data readiness:** Establishing a trusted, machine-readable data foundation that enables agents to evaluate, rank, and execute with confidence. This includes structured, prompt-aligned data across core domains such as product, pricing, promotions, inventory, fulfillment, and policy, supported by freshness, completeness, provenance, and explainability. Mature organizations advance from SEO to GEO to agentic commerce optimization (ACO), ensuring content and policies are designed for AI interpretation and agent-to-agent execution.
- **Technology and infrastructure readiness:** Delivering resilient, low-latency, and scalable platforms designed for autonomous, event-driven execution at machine speed. Prepared organizations architect systems for multi-step agent execution, supported by aligned technology platforms and systems integrator partnerships that accelerate time to value and reduce integration friction.
- **Trust, identity, and security readiness:** Enabling safe and scalable autonomy through verifiable agent identity, delegated authority, consent, and runtime policy enforcement. Advanced organizations move beyond traditional bot mitigation to agent aware cybersecurity, real-time observability, auditability, and failback mechanisms that preserve control, accountability, and resilience.
- **Operating model, processes, and talent readiness:** Embedding agentic commerce into day-to-day operations through clear ownership, cross-functional governance, redesigned workflows, and human-in-the-loop oversight. This includes disciplined change management, targeted talent upskilling and acquisition, and continuous feedback loops that allow agent-led execution to scale beyond pilots and deliver sustained business impact.

Figure 3: Dimensions of agentic commerce readiness



THE ROLE OF UNIVERSAL COMMERCE PROTOCOL (UCP)

The introduction of the UCP represents a significant inflection point in agentic commerce: it signals a shift to normalizing how intelligent agents discover, evaluate, and transact with merchants and brands across the open web. More than a technical standard, UCP positions agent-to-merchant interactions from proprietary pathways to a shared, scalable standard. By standardizing how product information, pricing, availability, policies, and transactions are exposed, UCP reduces fragmentation and shifts RCP organizations away from bespoke, point-to-point integrations and toward a more interoperable, protocol-driven model.

UCP reshapes default expectations of how businesses show up in agent-mediated commerce. As common patterns for discovery, verification, and execution become normalized, agents will increasingly favor organizations that are easy to understand, trustworthy to transact with, and seamlessly connected to the ecosystem. Organizations that align early could become frictionless participants in agent-driven flows, while those that delay risk reduced visibility and selection.

For retailers and brands, embracing UCP translates into four practical priorities:

1. **Get curious about your brand:** Understand how agents interpret your products, claims, and policies today—and where visibility or differentiation is limited.
2. **Invest in high-quality, original, structured content:** Ensure product information, specifications, and claims are authoritative, differentiated, and crawlable across the open web.
3. **Connect trusted agentic experiences:** Open branded experiences to selected agentic partners and enable secure, governed interactions through shared standards.
4. **Lean into Google Shopping and related surfaces:** Use UCP to connect shopping experiences across Google properties, ensuring consistent, agent-ready data and execution pathways.

UCP should not be viewed as a distant technical standard, but as an external forcing function accelerating ecosystem-wide alignment. When major platforms introduce foundational protocols, they do so with clear intent to operationalize, and organizations that delay risk being designed out of agent-driven commerce flows.

Figure 4: UCP overview

Consumer surfaces
e.g. AI Mode on Search, Gemini app and others

Universal Commerce Protocol (UCP)

Creates a common language for consumers, agents and businesses to ensure all types of commerce actions are standardized and secure

Capabilities and extensions

Agents and businesses have flexibility to choose which capabilities and extensions they adopt

Product discovery	**Cart**	**Identity linking**
Checkout	**Order**	**Other vertical capabilities**

Underlying communication

Enables merchants and agents flexibility to communicate in the medium of their choice

APIs	**Model Context Protocol (MCP)**	**Agent2Agent (A2A) Protocol**

Business backends
Process orders, manage inventory, arrange delivery

A PRACTICAL READINESS CHECKLIST AND A BROAD ROADMAP FOR LEADERS

Agentic commerce readiness is assessed through six dimensions, supported by Deloitte's framework and methodology for assessing RCP organizations. This includes ongoing maturity assessments for companies already on their agentic commerce journeys. While a full assessment is tailored to enterprise context, risk tolerance, and strategic objectives, the below framework provides examples of readiness attributes that are evaluated.

Preparing for agentic commerce should be approached in phases. Immediate actions focus on foundational capabilities that reduce risk and create optionality. Near-term efforts enable active participation in agent-led interactions. Longer-term investments support differentiation and agent-native execution.

Further, the journey to readiness requires clear leadership ownership: It should not be treated as a purely technical initiative or isolated innovation effort. Successful organizations will establish cross-functional governance that aligns commercial objectives with the right technology infrastructure, data, policies and security.

Figure 5: Diagnostic readiness checklist

Strategic vision	Data	Technology and infrastructure	Trust, identity and security	Operating model, process, talent
• Agentic commerce vision and ambition	• Machine readability and semantics	• Agent-ready execution platforms	• Agent identity and verification	• Workflow redesign and automation
• Executive sponsorship and decision rights	• Intent and prompt alignment	• Low-latency, scalable architecture	• Delegated authority and consent	• Governance and cross-functional coordination
• Business outcomes and value realization	• Freshness and real-time accuracy	• Event-driven interaction model	• Policy enforcement and scope control	• Exception handling and escalation (human-in-the-loop)
• Return on investment (ROI) tracking and key performance indicators (KPIs)	• Completeness and domain coverage	• SEO to GEO to ACO	• Cybersecurity and threat detection	• Talent upskilling, reskilling, acquisition
• Insight-to-action mechanisms	• Provenance and explainability	• Resilience and scalability	• Observability, auditability and telemetry	• Adoption and change enablement
	• Signal quality and authority	• Technology and partner ecosystem	• Failback and recovery procedures	• Measurement and control loops

CLOSING PERSPECTIVE

Agentic commerce is significantly reshaping the landscape for RCP organizations. The pace of change and adoption is exponential, and the value at stake is large: agents are already influencing outcomes (around ~20% of Black Friday 2025 sales were driven by LLMs[3]), and analysts predict that more than 25% of global retail sales will be completed by agents by 2030[4]. Readiness and speed will determine leaders. Regardless of where you are on the agentic commerce journey (e.g., nascent, aware, or well on your way to agent-native), a critical step you can take right now is to establish a clear baseline. Closing a gap you haven't measured is far more challenging than otherwise. You need to know your starting point to be able to track progress of your efforts and investments. Assess where your organization stands across data, technology, trust, and operating model dimensions today, so that the distance between where you are and where you need to be becomes a roadmap. Organizations that invest in readiness now are likely better positioned to shape agent behavior, protect margin, and maintain visibility as commerce execution evolves. As agentic solutions mature, the catch-up curve steepens: leaving late movers exposed to increased competitive pressure, performance gaps, operational inefficiencies, and heightened compliance and control risk.

AUTHORS

Saurabh Vijayvergia
Deloitte Consulting LLP
svijayvergia@deloitte.com

Brian McCarthy
Deloitte Consulting LLP
brimccarthy@deloitte.com

Kapil Dabi
Google Cloud
kapildabi@google.com

Sonia Fife
Google Cloud
sonfife@google.com

KEY CONTRIBUTORS

Gagan Mehra
Deloitte Consulting LLP
gaganmehra@deloitte.com

Niladri Gupta
Deloitte Consulting LLP
nilgupta@deloitte.com

Tye Chait
Deloitte Consulting LLP
tchait@deloitte.com

Jonathan Cherepanov
Deloitte Consulting LLP
jcherepanov@deloitte.com

Ana Musson
Deloitte Consulting LLP
amusson@deloitte.com

ENDNOTES

1. eMarketer, 'Over half of US consumers intend to use genAI when shopping online this year' (2025)
2. Google, "New tech and tools for retailers to succeed in an agentic shopping era" (January 2026)
3. Business Insider, 'How AI is silently becoming the holiday shopper's secret weapon' (2025)
4. Wall Street Journal, 'Agentic Commerce: Strategic Implications for Retail Brands' (2025)