When agents become the customer: Architecting commerce infrastructure for autonomous AI buyers

A Thoughtworks strategic briefing

Author: Rav Hayer, Managing Director, UK and Ireland;
Head of BFSI Europe, Thoughtworks

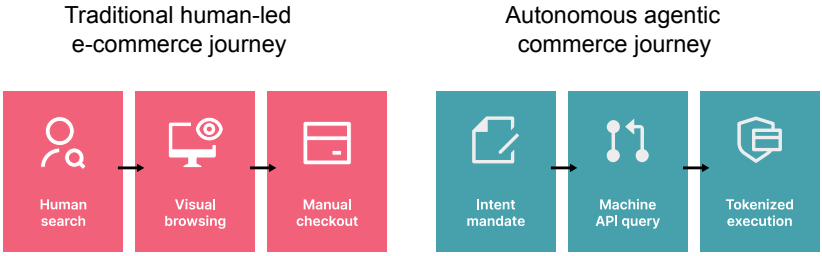
/thoughtworks

Design. Engineering. AI.

Executive summary

Digital commerce is experiencing its most significant structural shift since the launch of the commercial internet. For three decades, enterprise commerce architectures have been designed around a single operational model: optimizing human visual engagement. Organizations have invested heavily in visual interfaces, cart conversion and personalized marketing journeys.

That model is now changing. Commerce is moving from manual human browsing toward delegated, autonomous machine execution. Research projects that AI agents will drive up to 25% of global e-commerce volume by 2030, representing $115 billion in added value in the US market alone, as nearly 50% of online shoppers adopt AI proxies. Meanwhile, 60% of consumers expect to use AI agents within the next year, and 73% are already using AI tools for product discovery, price comparison and review summaries.



Legacy commerce stacks remain built for human interaction. When an autonomous AI agent tries to discover products, evaluate options, authenticate identity, execute payments or process returns, traditional systems create friction. AI does not fix poor infrastructure. It amplifies it. Inconsistent product data leads to unreliable AI recommendations, siloed fulfillment causes fragmented execution and disconnected checkout flows accelerate abandonment.

This paper sets out an updated strategic framework for leaders across retail, marketplaces, travel and financial services. It outlines the technical, operational and architectural requirements for turning enterprise digital cores into machine-readable, protocol-agnostic engines that can serve both human shoppers and autonomous AI agents.

1 The core paradigm shift: from human clicks to delegated buying

Agentic commerce marks the evolution of artificial intelligence: from passive recommendation engines that predict what a human might select, to delegated operational surrogates that execute purchases within explicit parameters.

The decline of visual interface dominance

Traditional digital marketing relies on influencing human emotion through visual brand presentation, promotions and guided browsing paths. An autonomous software agent, by contrast, evaluates products using structured utility functions: objective pricing, verified material specifications, real-time inventory depth, fulfillment speed and explicit return policies.

If product catalogs sit behind unstructured web pages and client-side scripts with no machine-readable data layer, autonomous agents will bypass those storefronts for accessible alternatives. Retailers without machine-first integration layers risk being pushed into the role of back-end supplier.

The dual dynamics of discovery: owned versus third-party agents

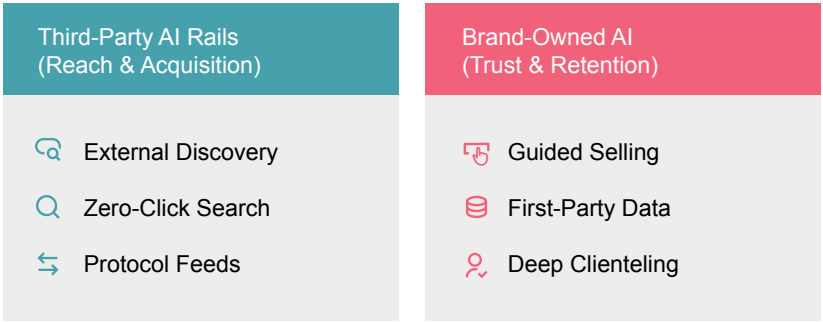
The shift toward agent-mediated discovery creates a dual strategy for commerce brands:

- **Third-party AI environments:** Platforms such as ChatGPT, Google Gemini and Microsoft Copilot act as external discovery

gatekeepers. Capturing demand here requires structured metadata, real-time API access and compliance with emerging agentic protocols.

- **Brand-owned conversational environments:** Guided selling experiences powered by generative AI within a brand's own web or mobile applications let retailers keep direct customer relationships, offer personalized guidance using proprietary data and reinforce brand loyalty.

Agentic commerce dual growth engine



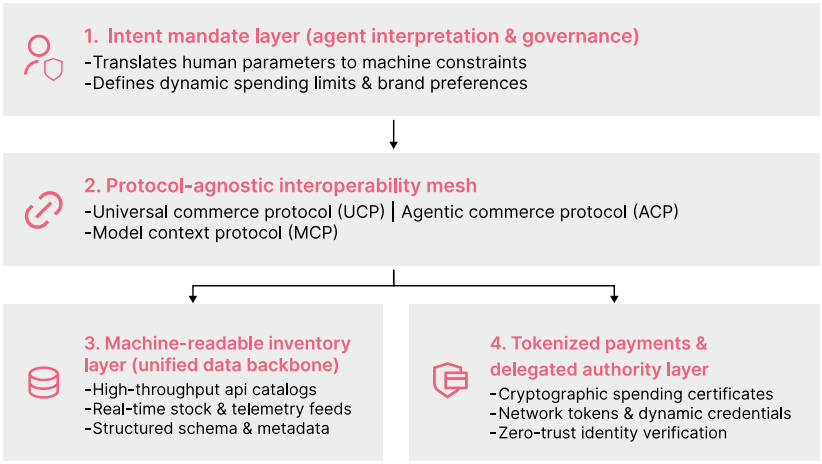
The loyalty paradox and algorithmic evaluation

When AI agents act as intermediaries, consumer reliance on direct brand domains changes. If an agent weighs objective utility over historical brand affinity, generic or challenger competitors gain immediate visibility. To hold their market position, merchants must structure product quality metrics, ethical sourcing data and fulfillment reliability scores so machine algorithms can evaluate them.

2 Technical architecture: machine-readable data, multi-protocol fabrics and agentic payments

Moving to an agentic commerce model requires updating data exposure layers, identity frameworks, payment mechanics and protocol integration.

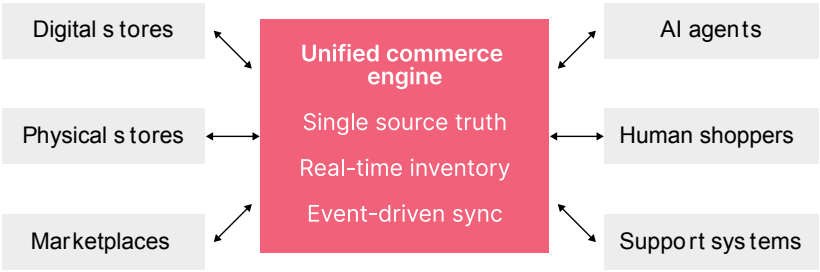
Modern agentic commerce infrastructure matrix



Unified commerce as the data foundation

AI agents need structured, reliable information: accurate pricing, real-time inventory availability across locations and consistent product metadata. Fragmented data leads to miscalculated stock, broken recommendations and failed transactions. Unified commerce is the core layer here: a single source of truth for product, price and inventory data across digital storefronts and physical locations.

Unified commerce architecture: data foundation for agentic commerce



Protocol-agnostic integration layer

Enterprise architecture should support multiple emerging standards so AI models, merchant platforms and payment networks can communicate:

- **Model Context Protocol (MCP):** Standardizes structured context exchange between AI models and enterprise tools. Lets agents query catalogs, carts and customer context safely, without executing direct financial transactions.
- **Agentic Commerce Protocol (ACP):** Connects AI agents, such as those in the OpenAI/ChatGPT ecosystem, directly to merchant systems and payment providers, such as Stripe, to run cart management and checkout flows.
- **Universal Commerce Protocol (UCP):** An open standard that unifies transaction signals, discovery query formats and capability negotiations across merchants, agents and payment rails.

Rather than build custom point-to-point integrations for each standard, organizations can deploy an abstraction layer that translates internal APIs into MCP, ACP or UCP formats as needed.

API-first modularity and high-throughput scaling

Traditional platforms built for human browsing traffic can hit performance bottlenecks when they meet automated queries. AI agents issue high-frequency API calls to check stock across item variants, compare real-time pricing and validate delivery options in milliseconds.

A modular, API-first architecture decouples core commerce functions, such as cart, pricing, inventory and checkout, into independently scalable services. Event-driven architectures keep inventory updates and price changes synchronized instantly across all touchpoints, without slowing checkout performance.

Delegated authority and tokenized payments

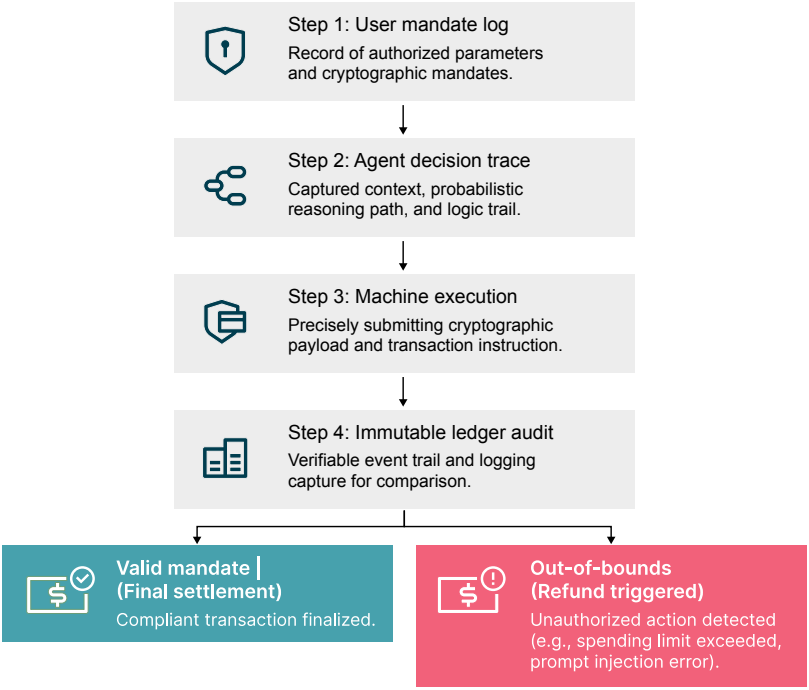
Autonomous purchases skip traditional human verification steps, such as manual card entry or two-factor authentication (2FA) prompts. Secure agentic transactions rely on dedicated delegation mechanisms:

- **Cryptographic mandates:** Users issue time-bound digital certificates that set explicit spending caps, merchant categories and product constraints for their agents.
- **Network tokenization:** Transactions run on dynamic, tokenized payment credentials bound to verifiable agent identities, avoiding the transmission of raw primary account numbers (PANs).
- **Tiered autonomy:** Customers give agents full execution authority for routine, low-value purchases, while keeping manual approval requirements for high-value or unusual transactions.

3 Disputes, governance and multi-party liability models

When an autonomous agent buys the wrong item, exceeds its instructions or runs into a malicious prompt injection, traditional chargeback mechanisms and consumer protection frameworks need to adapt.

Dispute governance and multi-party liability model



Potential failure modes

- **Out-of-mandate execution:** The agent completes a purchase that exceeds authorized spending limits or conflicts with the user's stated preferences.
- **Prompt injection and data poisoning:** Malicious actors manipulate unstructured product metadata or third-party web content to alter an agent's product selection logic.
- **System duplication:** Network timeouts or protocol mismatches cause duplicate order instructions to process.

Reconstructing the evidentiary trail

Resolving transaction disputes requires an immutable, step-by-step audit trail that captures four primary events:

- **The intent mandate:** The verifiable record of authorized user constraints and spending parameters.
- **The environmental context:** The real-time pricing, stock availability and product specifications presented to the agent at the time of decision.
- **The decision trace:** The probabilistic reasoning path or logic sequence the AI agent generated.
- **The execution instruction:** The cryptographic transaction payload submitted to the payment gateway.

Liability models will move beyond binary merchant-versus-issuer chargeback structures, toward shared accountability models that involve agent developers, identity issuers, protocol providers and merchants.

4 Industry case studies: foundational readiness in action

Leading enterprises across sectors show how modular infrastructure and unified data systems enable real-time execution across channels.

JD Sports: preparing for one-click AI commerce

Global sports fashion retailer JD Sports updated its commerce stack with composable architecture to support direct purchases within AI environments.

- **The strategy:** Integrates inventory across its brand portfolio, including JD, DTLR, Shoe Palace and Hibbett, to enable real-time search, stock checks and checkout through AI platforms such as Microsoft Copilot, Google Gemini and OpenAI's ChatGPT.
- **The architecture:** Combines composable commerce capabilities from commercetools with Stripe's payment infrastructure, letting customers complete transactions natively inside AI conversational interfaces.
- **Key takeaway:** Modular APIs let brands make their product catalogs transactional across external AI channels, without adding operational complexity to back-end systems.

Screwfix: omnichannel cart and order synchronization

Screwfix, a UK supplier for tradespeople, built a unified commerce architecture to deliver consistent customer experiences across digital and physical touchpoints.

- The strategy: Synchronizes real-time cart and inventory logic across mobile apps, web storefronts and in-store digital tablets.
- The architecture: Uses a modular commerce core that lets product teams deploy new payment methods and checkout features independently. Customers can build order baskets online or via in-store tablets and complete pickup transactions at the counter with live stock validation.
- Key takeaway: Unifying cart management and inventory logic across channels builds the operational groundwork needed to process high-speed queries from both human shoppers and AI agents.

Pet Valu: automation and full-catalog visibility

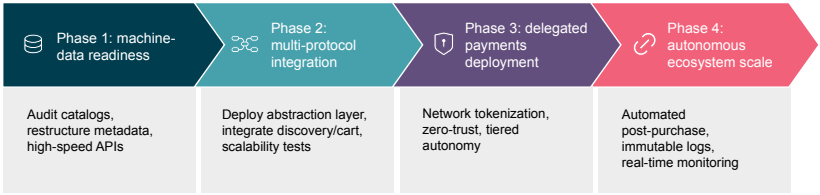
Pet Valu, which operates over 800 stores across Canada, updated its legacy technology to remove catalog restrictions and automate promotional logic.

- The strategy: Resolved fragmented regional inventory visibility and manual promotion deployment across its store network.
- The architecture: Implemented a centralized, API-first commerce engine that automates promotion distribution and exposes the complete product catalog across all regions and digital channels.
- Key takeaway: Exposing complete, machine-readable catalog and promotion data is essential for letting AI agents evaluate and apply the right discounts accurately.

5 Enterprise production roadmap: moving beyond AI pilots

Moving from isolated AI pilots to a production-ready commerce architecture involves four main phases.

Agentic commerce: enterprise production roadmap



Phase 1: machine-data readiness and unification

- Audit enterprise catalogs, pricing rules and inventory systems to establish a single source of truth.
- Restructure product metadata, material specs and fulfillment parameters into structured formats.
- Expose key data points through high-speed, lightweight APIs that can handle automated query traffic.

Phase 2: multi-protocol integration

- Deploy an abstraction layer that supports emerging agentic commerce protocols, including MCP, ACP and UCP.
- Integrate discovery and cart management flows across third-party AI channels and brand-owned conversational interfaces.
- Test system performance under simulated high-frequency API traffic to confirm scalability.

Phase 3: delegated payment deployment

- Partner with payment processors to support network tokenization, dynamic payment credentials and cryptographic spending limits.
- Implement zero-trust identity verification frameworks to authenticate agent instructions.
- Configure tiered autonomy controls that let users set explicit spending thresholds for automated execution.

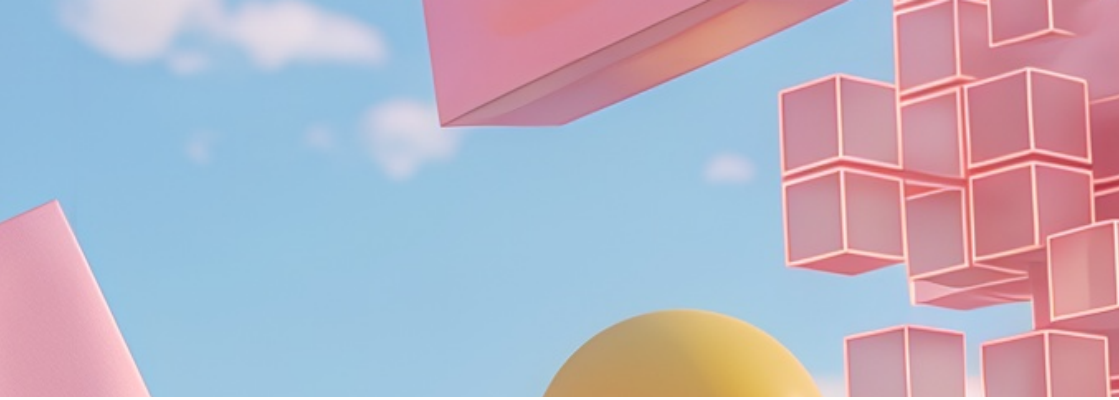
Phase 4: autonomous ecosystem scale

- Extend agentic workflows into post-purchase processes, including automated order tracking, proactive replenishment and return processing.
- Implement immutable logging infrastructure to track intent mandates, context state and execution payloads for dispute resolution.
- Establish real-time monitoring to track conversion rates, API performance and transaction accuracy across agent channels.

Executive strategic checklist

Before expanding agentic commerce initiatives, executive leadership should assess organizational readiness across three core areas:

1. **Data accessibility and structure:** Are product catalogs, real-time inventory counts and pricing rules accessible through structured, machine-readable APIs that external AI agents can query efficiently?
2. **Payment infrastructure and delegated authority:** Can your current payment architecture validate cryptographic spending mandates, process network tokens and complete checkout flows without requiring real-time human interaction?
3. **Auditability and dispute governance:** Do you maintain immutable logging systems that can record agent decision traces, environmental context and user mandates, to resolve out-of-bounds purchase disputes?



References

[Ref-1] Thoughtworks executive briefing: When Agents Become the Customer: Architecting Commerce Infrastructure for Autonomous AI Buyers.

[Ref-2] commercetools industry report: Reimagining Retail in 2026: Building the Retail Foundation for Agentic Commerce and Everything Beyond.

To discuss how Thoughtworks can help your organization update its digital core and build secure agentic commerce capabilities, contact Rav Hayer or the Thoughtworks Financial Services and Retail practice.

For more than 30 years, Thoughtworks has helped shape how the world builds technology.

Today, by harnessing AI to scale what is possible, guided by human judgment and experience, we aim to be the force behind the world's most consequential technology transformations.

We combine our engineering and design expertise with AI to modernize systems, unlock data and create AI-powered products.

AI/works™ is our agentic development platform and Agent/works™ is our enterprise platform for governing and running autonomous AI agents. Together they bring decades of our engineering know-how to every stage of AI software delivery, from development through to deployment and governance.

thoughtworks.com

/thoughtworks

Design. Engineering. AI.

Last updated September 2026