

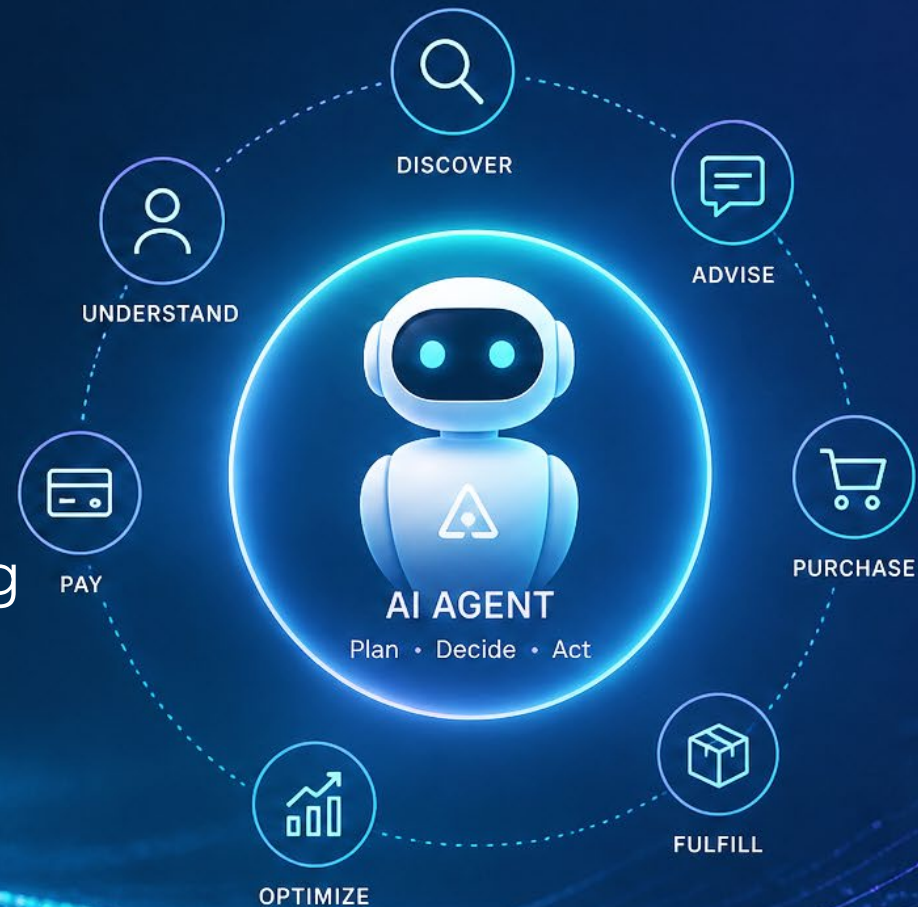


In partnership with



Agentic Commerce Playbook:

A Step-by-Step Framework for Retail Implementation and Scaling



June 10, 2026

Copyright © 2026 Coresight Research. All rights reserved.

Executive Summary

Retailers should adopt a **tiered strategy**, prioritizing GEO and structured product feeds as foundational capabilities. In the near term, visibility will be the most critical battleground. As AI agents increasingly mediate discovery and purchase, retailers that fail to structure product data or optimize for AI engines risk becoming invisible in consumer journeys. Coresight Research's STORE framework—strategy, technology, operations, risk and resilience, and ethics—helps retailers plan their approach to agentic commerce in a more structured way, identify the relevant technology partners, set up practical operating processes, manage risk and adopt AI responsibly.

What We Think

Agentic commerce marks the beginning of a **new operating model for retail**, where success depends on participation in AI ecosystems, excellence in data and operations, and the ability to balance innovation with trust. Retailers that take a phased, disciplined approach—grounded in ROI and supported by strong governance—will be best positioned to capture value as this model scales.

Coresight Research Analysis: The STORE Framework

Strategy: A Staged Approach to Agentic Commerce Adoption

Retailers should adopt agentic commerce through a phased strategy, beginning with generative engine optimization (GEO) and structured product feeds to ensure visibility, followed by conversational checkout and, eventually, proprietary AI agents. Each phase adds value, but it also requires more investment and stronger capabilities across the organization.

Technology: Data and Interoperability as the Foundation

Agentic commerce depends on a unified, API-driven technology stack built on structured, real-time data. Retailers need systems that work well together so AI agents can find products, evaluate options and complete transactions without friction.

Operations: Implementation Through Structured Execution

Adoption works best when retailers roll out agent-driven capabilities incrementally. This requires clear ownership, defined use cases and infrastructure that can support live agent activity and fulfillment.

Risk and Resilience: Managing Autonomous System Risks

As AI agents take on more responsibility, retailers face new risks, from fraud and data exposure to unintended actions taken by automated systems. A layered security approach, supported by monitoring and human oversight, is essential to keep systems stable and trustworthy.

Ethics: Building Trust Through Governance and Transparency

Trust will determine the pace of adoption. Retailers need to build transparency and accountability directly into their systems, with clear rules around data use, safeguards to address bias and defined points where humans remain in control.

Contents

Introduction	4
Market Scale and Opportunity	6
Agentic Commerce Playbook: A Step-by-Step Framework for Retail Implementation and Scaling .	7
Strategy: Choosing the Right Agentic Approach	8
Technology: Building the Agentic Stack Aligned to Strategy	11
Operations: How to Implement Agentic Commerce	16
Risk and Resilience: Security Risks and Systemic Integrity	21
Ethics: Trust, Fairness and Societal Impact	24
What We Think	26
Implications from This Report.	28
Implications for Brands and Retailers.	29
Implications for Technology Vendors	30
Notes and Methodology	31
About Coresight Research Custom Reports	32
About Rezolve Ai	32

Introduction

This playbook translates the emerging state of agentic commerce into concrete actions for retailers. Agentic commerce marks the next phase in the evolution of digital retail, shifting from user-driven interactions to AI-mediated shopping journeys. Unlike traditional e-commerce, where consumers search for, compare and purchase products directly, agentic commerce enables AI agents to act on behalf of users, discovering products, evaluating options and completing transactions within a single conversational flow.

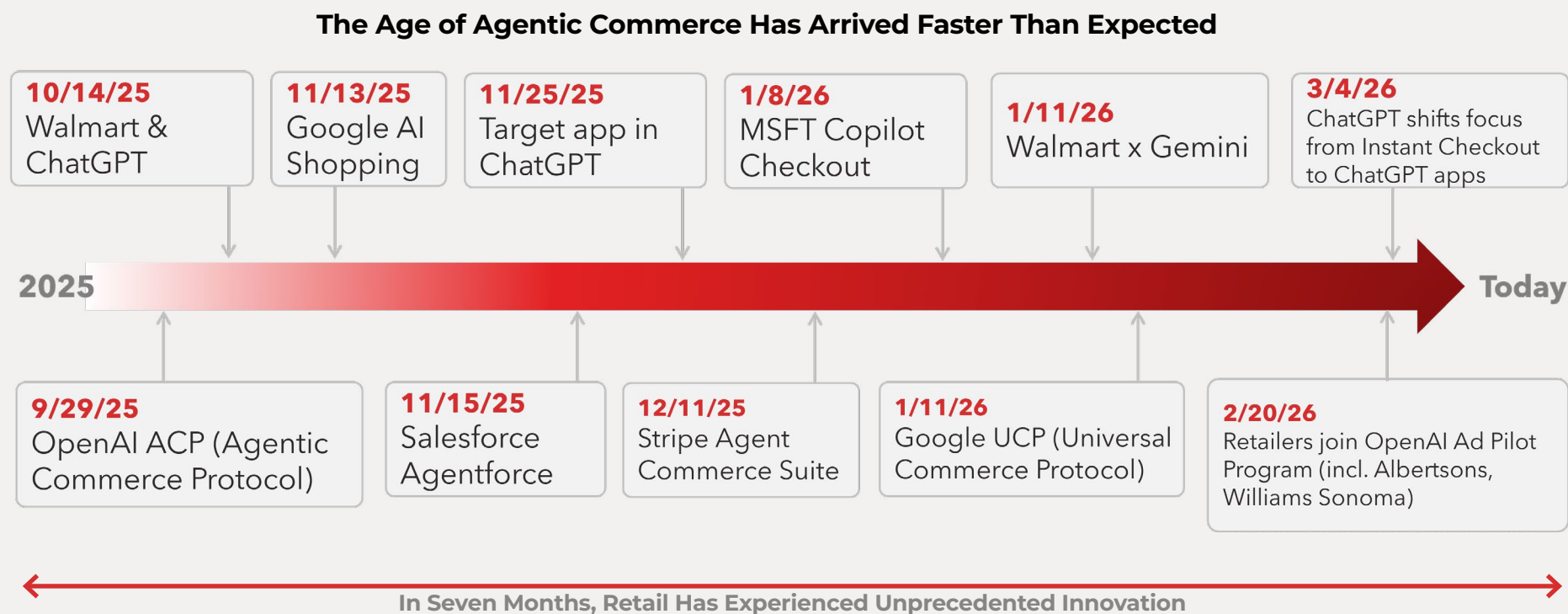
This shift is driven by advances in agentic AI and the rapid adoption of AI-powered conversational interfaces. Platforms such as ChatGPT and Google Gemini are increasingly integrating shopping capabilities, enabling consumers to move seamlessly from intent to purchase without leaving the AI environment. As a result, the traditional retail funnel—awareness, consideration and conversion—is collapsing into a unified experience.

For retailers, this transformation presents both opportunities and challenges. On one hand, agentic commerce offers the potential to improve conversion rates, enhance personalization and streamline customer experiences. On the other hand, it disrupts established models of traffic acquisition, customer engagement and data ownership. Retailers must now ensure that their products are visible and accessible within AI ecosystems, rather than relying solely on their own digital channels.

This report provides a comprehensive playbook for retailers to navigate this shift. It outlines the strategic approaches, supporting technologies, operational requirements, risk considerations and ethical frameworks needed to capture value while managing complexity and risk in an increasingly AI-driven retail environment.

This report is made available to nonsubscribers of Coresight Research in partnership with **Rezolve Ai**, a leading provider of commerce-led solutions.

Figure 1.
The Arrival of Agentic Commerce



Source: Coresight Research

What Is Agentic Commerce?

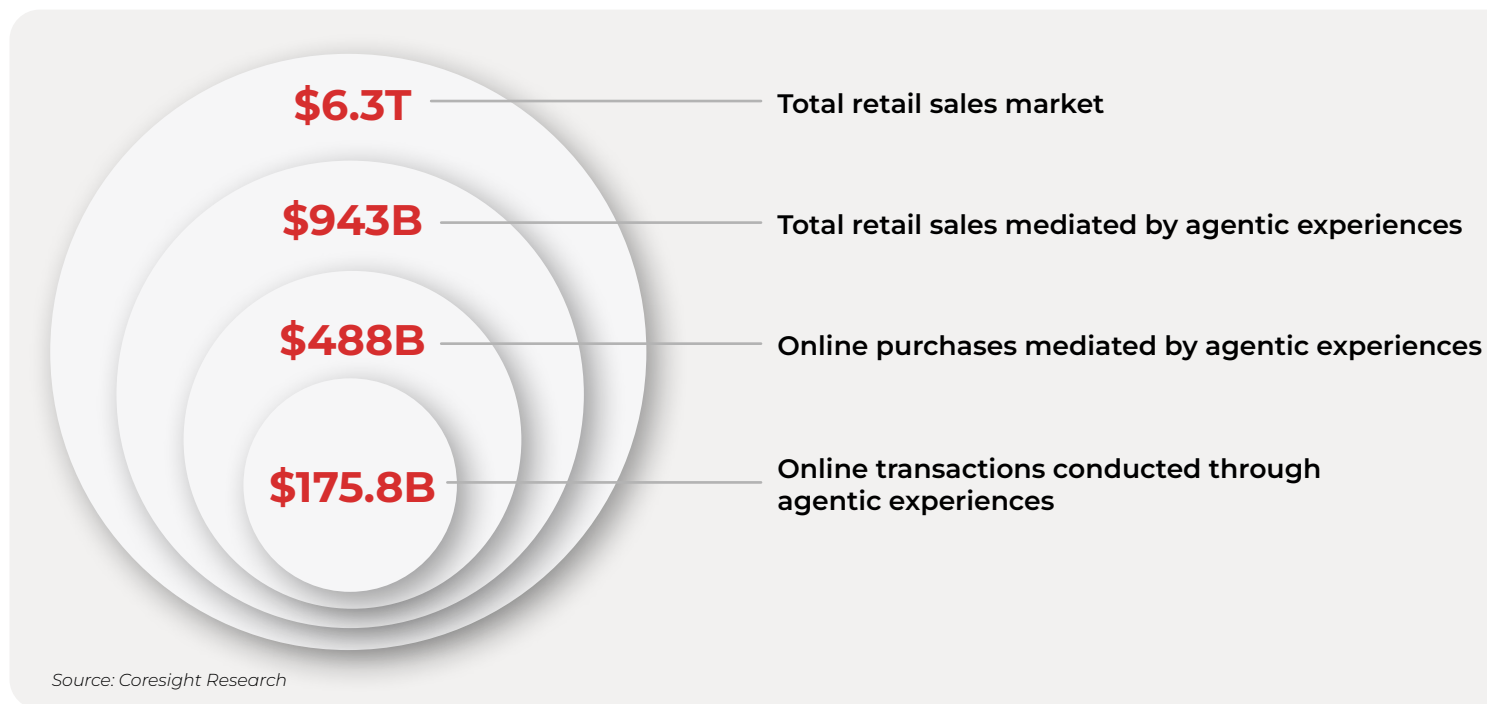
Agentic commerce refers to a new shopping model in which AI agents act on behalf of consumers to discover products, compare options across brands and retailers, and complete purchases within a single, unified flow. Instead of consumers browsing individual websites or apps, they can delegate intent—such as “create a cart for my weekly shopping list”—to an AI agent. The agent then sources products across multiple brands, retailers and private labels, aggregates them into a single cart, and executes the transaction through integrated checkout systems such as ChatGPT’s Instant Checkout or Google’s Universal Commerce Protocol (UCP).

This model fundamentally changes the structure of retail. The customer interacts primarily with the AI agent, while retailers and brands compete behind the scenes for inclusion in the agent’s recommendations and final purchase decision. As a result, the shopping journey becomes less fragmented and more outcome-driven, with discovery, decision-making and checkout collapsed into a single interaction.

Market Scale and Opportunity

Agentic Commerce experiences are reshaping the retail industry. According to Coresight Research estimates, the US agentic commerce market will reach \$943 billion by 2030, which includes total retail sales mediated by agentic experiences that ultimately result in a transaction.

Figure 2.
US Agentic Commerce Market Size by 2030 (USD Bil.)



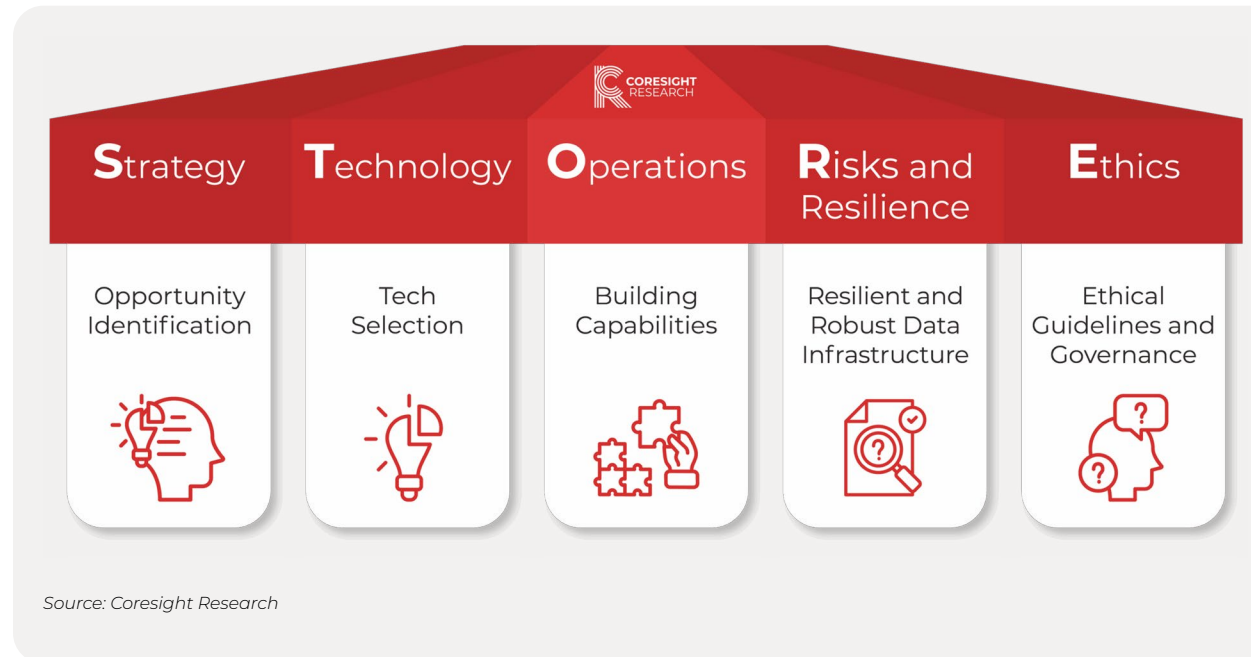
*Note: Online transactions **conducted through** agentic experiences refers to retail transactions (purchases of goods) completed by, or directly as a result of, AI-powered agents and platforms. This includes: (1) purchases made on a retailer's or brand's website immediately following and directly related to a click-through from a third-party platform such as ChatGPT and Gemini (off-site checkout); (2) transactions fully completed on those third-party platforms (on-site checkout); (3) transactions made through retailers' and brands' own AI-powered agents such as Buy for Me (Amazon); (4) transactions fully executed by an AI agent on a shopper's behalf.*

*Total retail sales **mediated by** agentic experiences refers to any retail transaction influenced by a Generative AI agent. This includes but is not limited to: (1) product or service search results during any stage of the consumer purchase journey; (2) retailer choice influenced by Agentic recommendations.*

Agentic Commerce Playbook: A Step-by-Step Framework for Retail Implementation and Scaling

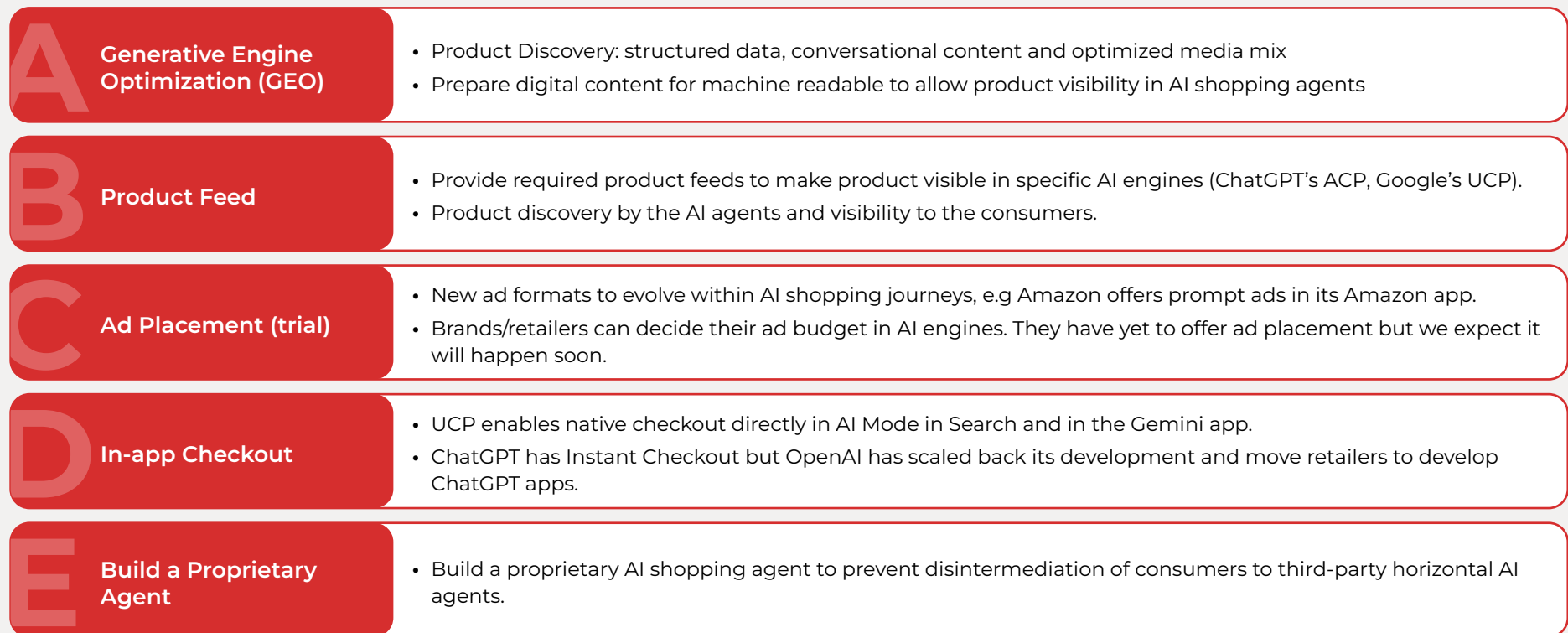
- **Strategy:** Retailers should adopt a staged, ROI-driven approach, starting with GEO and product feeds to ensure visibility, then progressing to conversational checkout and proprietary agents to ensure competitiveness in AI-driven commerce, given resources and ROI are considered feasible.
- **Technology:** Agentic commerce requires a technology stack built on structured data, real-time integrations and interoperable platforms that enable AI agents to discover, decide and transact seamlessly.
- **Operations:** Retailers should implement agentic commerce with clear steps across product feeds, conversational checkout, GEO and proprietary agents.
- **Risks and Resilience:** Retailers must implement layered security, continuous monitoring and governance controls to manage emerging risks across data, systems and autonomous decision-making.
- **Ethics:** Coresight Research provides the approach to embed transparency, accountability and human oversight across the full AI lifecycle to ensure secure and responsible agentic commerce.

Figure 3.
Coresight Research STORE Framework for Driving Innovation in Retail



Retailers should adopt a tiered approach to agentic commerce based on their resources, data maturity and customer objectives. The options—generative engine optimization (GEO), structured product feeds, agentic checkout via the Agentic Commerce Protocol (ACP), the Universal Commerce Protocol (UCP) and ChatGPT apps, and building a proprietary AI shopping agent—are not mutually exclusive but rather sequential building blocks. A clear ROI framework helps determine which combination to pursue.

Figure 4.
A Tiered Approach to Enabling Shoppability on Conversational AI Engines



Source: Coresight Research

Figure 4 shows the five-tiered approach for retailers to implement agentic commerce. GEO and Product Feed are responsible for consumers' product discovery. In-app checkout aims to bring the transaction directly into AI agents. Retailers that have the resources can consider developing their own proprietary shopping agents so that the data and interactions with consumers are retained. The tiers below reflect a progression from visibility and discovery to transaction and ownership:

- A** Enable AI-friendly discovery through GEO. GEO involves tailoring content and metadata so AI agents can understand and prioritize products. AI shopping agents prioritize structured, verified data with human-readable content. Retailers should move beyond keyword-based SEO to conversational language and structured schema, aligning product descriptions with likely consumer questions. AI engines rely heavily on earned media—authoritative third-party reviews and news—while placing less weight on brand-owned and social content; thus retailers should cultivate credible external coverage to boost AI visibility. GEO is the entry point and a prerequisite for higher tiers.
- B** Expose products to conversational AI through structured product feeds via ACP and UCP. OpenAI's ACP and Google's UCP allow retailers to submit structured product feeds containing IDs, titles, prices, availability and images. Sellers push feeds to agreed endpoints, can update them every 15 minutes. Providing feeds ensures visibility to AI agents for matching and reduces reliance on web scraping. For small sellers, platforms like Etsy and Shopify automatically feed product data into ChatGPT. This approach offers quick visibility with minimal technical overhead.
- C** Prepare for ad placement (trial). Deploy targeted paid advertising within AI platforms to ensure discoverability and measure the effectiveness of agentic commerce. While AI engines have yet to offer ad placement, we expect this to happen in the short term, with Amazon offering prompt ads at no cost during its trial stage. Retailers can plan and allocate their ad budget in advance alongside GEO and product feeds to maintain visibility. This no-cost trial stage also allows brands to experiment with AI-native ad formats (e.g., sponsored responses or conversational ads) and refine messaging based on early performance.
- D** Move transactions into AI interfaces through conversational checkout. Conversational checkout collapses the purchase process into a conversational flow. Google's UCP offers native checkout across Search AI Mode and the Gemini app, requiring a checkout API conforming to the UCP state machine. ChatGPT's ACP requires retailers to build an Agentic Checkout API supporting create/update/delete states, and integrate payments via Stripe or PayPal. However, OpenAI has announced that it will scale back on Instant Checkout and instead encourage retailers to opt for ChatGPT apps to enable in-app checkout and multi-item purchases. Retailers should decide their approach in conversational checkout for AI-native shoppers.
- E** Retain control and data by building a proprietary AI shopping agent. Owning the conversational channel can safeguard first party data and monetization. Amazon's Rufus, embedded within its platform, engages more than 250 million customers and increases conversion by over 60%, according to Amazon's announcement in November 2025. Walmart launched its Sparky agent and simultaneously partnered with OpenAI and Google to integrate Instant Checkout. Building a proprietary agent makes sense for large retailers with scale, deep loyalty data and the resources to develop secure AI infrastructure. Smaller retailers should partner with third party agents and focus on data quality and integration rather than building from scratch.

ROI Considerations and When to Adopt

Early agentic initiatives show promising returns: consumers using AI assistants convert at significantly higher rates, AI-enabled planning and replenishment reduce stockouts and free working capital, and unified AI planning improves inventory turnover and reduces markdowns. Retailers should start with GEO and product feeds, which require modest investment and provide quick visibility, then evaluate the ROI of Instant Checkout through pilot tests. Building a proprietary agent should be justified by the value of retaining customer data and the scale of potential transactions. Measuring metrics such as conversion uplift, basket size and retention will inform the decision.

Figure 5.
The ROI Framework for Agentic Commerce

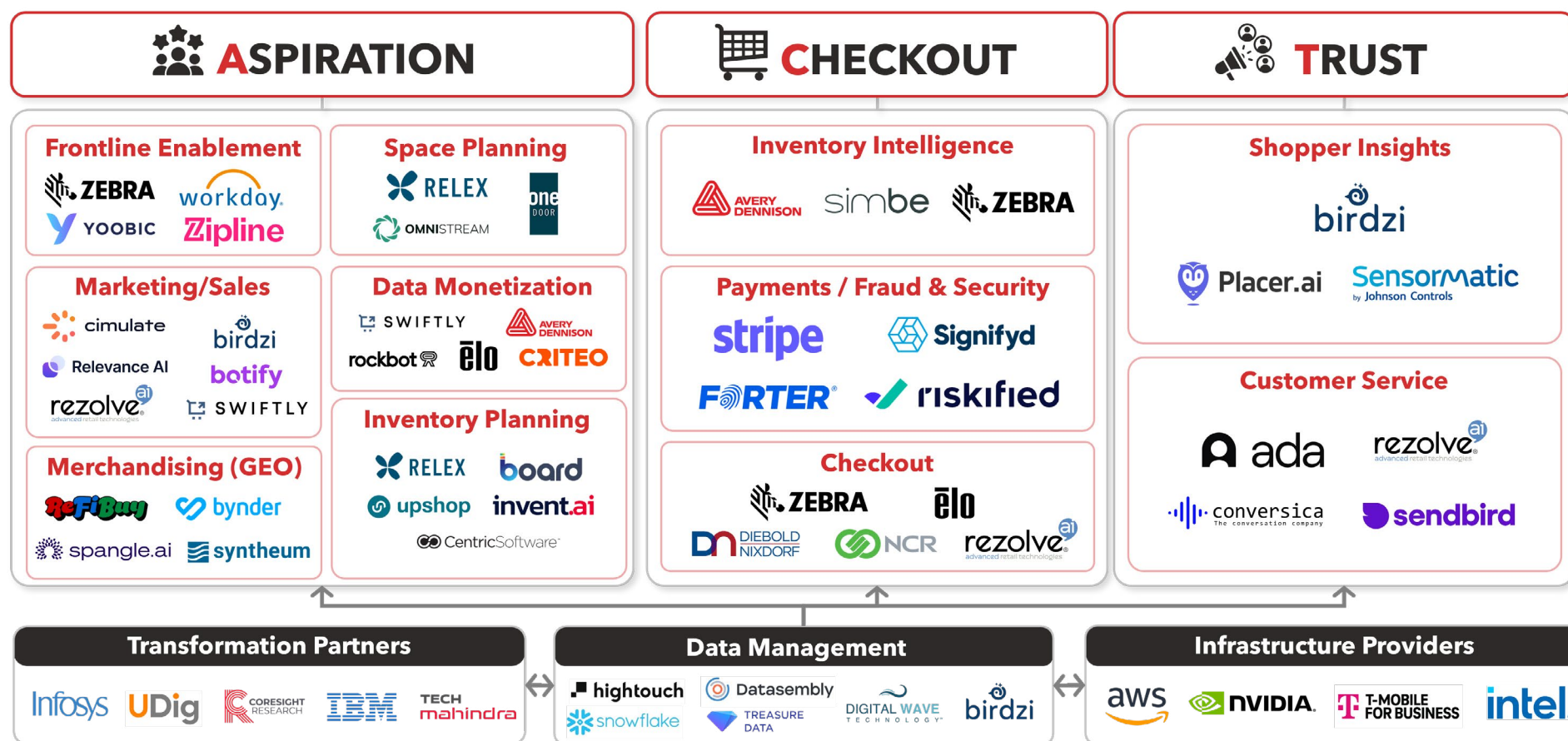
Step	Detail
1. Define Success	Align agentic KPIs with core revenue and productivity goals.
2. Establish the Baseline	Audit preagentic performance across sales and labor costs.
3. Project AI Gains	Estimate lift from instant checkouts, GEO and conversational ads.
4. Assess Implementation Costs	Account for API integrations, agent development and data prep.
5. Value Intangible Benefits	Factor in brand reputation and long-term customer loyalty.
6. Set a Realistic Horizon	Phase your ROI expectations from quick wins to long-term R&D.
7. Model the “Do Nothing” Scenario	Quantify the opportunity cost of bypassing agentic channels.
8. Calculate Total ROI	Run the final numbers comparing agentic lift against total investment.
9. Monitor and Iterate	Continuously optimize agent behavior to maximize conversion.

Source: Coresight Research

2 Technology: Building the Agentic Stack Aligned to Strategy

Coresight Research has introduced the Agentic Commerce Enablement Ecosystem, which includes companies that help retailers at three stages of the consumer journey: Aspiration, Checkout and Trust (ACT). These companies work with transformation partners, data management providers and infrastructure providers. Aspiration includes the service providers for product discovery, GEO and the relevant operations support; checkout comprises inventory intelligence, transaction execution, payments and security; and trust includes shopper insights and customer service support.

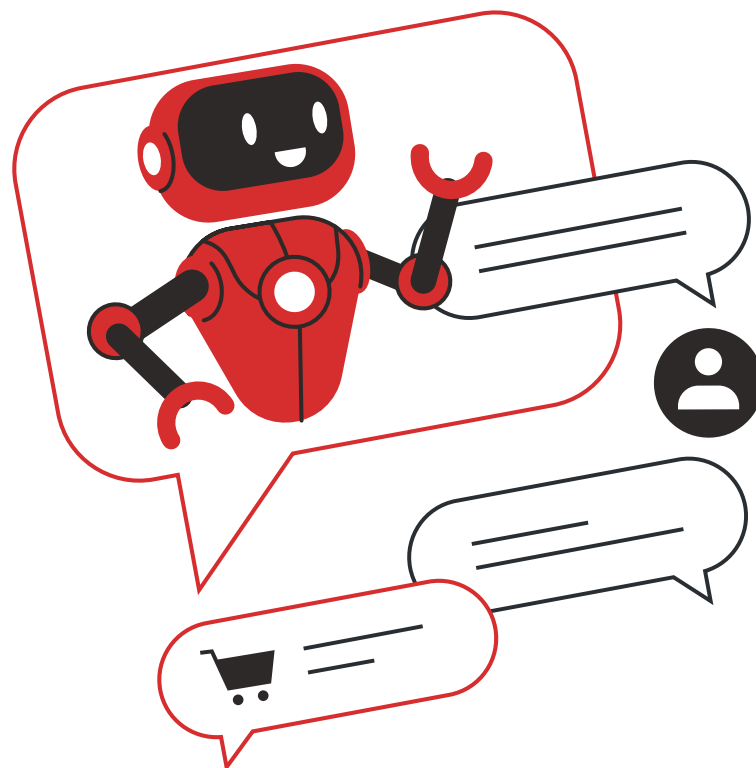
Figure 6.
The Agentic Commerce Enablement Ecosystem—Aspiration, Checkout and Trust (ACT)



Source: Coresight Research

The technology roadmap should align with the chosen strategy tier—GEO, product feeds, conversational checkout or proprietary agent. It spans data infrastructure, AI partner integrations and operational tools. Vendors across categories (frontline enablement, marketing, merchandising, inventory, payments and fraud) must provide APIs and data models that feed agents and support real-time interactions. The technologies below reflect how these needs differ by tier:

- **Technologies for GEO and product feeds.** GEO relies on content management systems that support schema markup, conversational copy and earned media monitoring. Providers such as Digital Wave Technology enable content management that underpins GEO and feeds. Salesforce's Agentforce Commerce manages ACP alignment for large retailers. Vendors like RELEX, Board and Centric Software enable inventory planning that provides the back-end intelligence to support agentic promises.
- **Technologies for conversational checkout.** Implementing agentic checkout requires real-time APIs for product data, pricing, tax, shipping options and order status. Stripe's shared payment token underlies ACP payments, while PayPal and Adyen are integrating with UCP. Retailers must integrate order management and inventory systems so AI agents can fetch availability and update reservations.
- **Technologies for proprietary agents and advanced capabilities.** Retailers building their own agents require natural-language understanding, recommendation and dialogue management capabilities. Amazon's proprietary agent stack (Rufus and Buy for Me) uses the company's vast catalog and user data. Walmart's Sparky uses AI to curate gifts and reorder groceries. These agents rely on data platforms, vector databases for semantic search, generative models and reinforcement learning with human feedback. Retailers should work with transformation partners (e.g., Tech Mahindra and UDig offer tech consulting services), data management providers (e.g., Snowflake and Treasure Data) and infrastructure providers (T-Mobile, NVIDIA and AWS provide the foundation for agent development) to develop in-house models to secure agentic interactions.



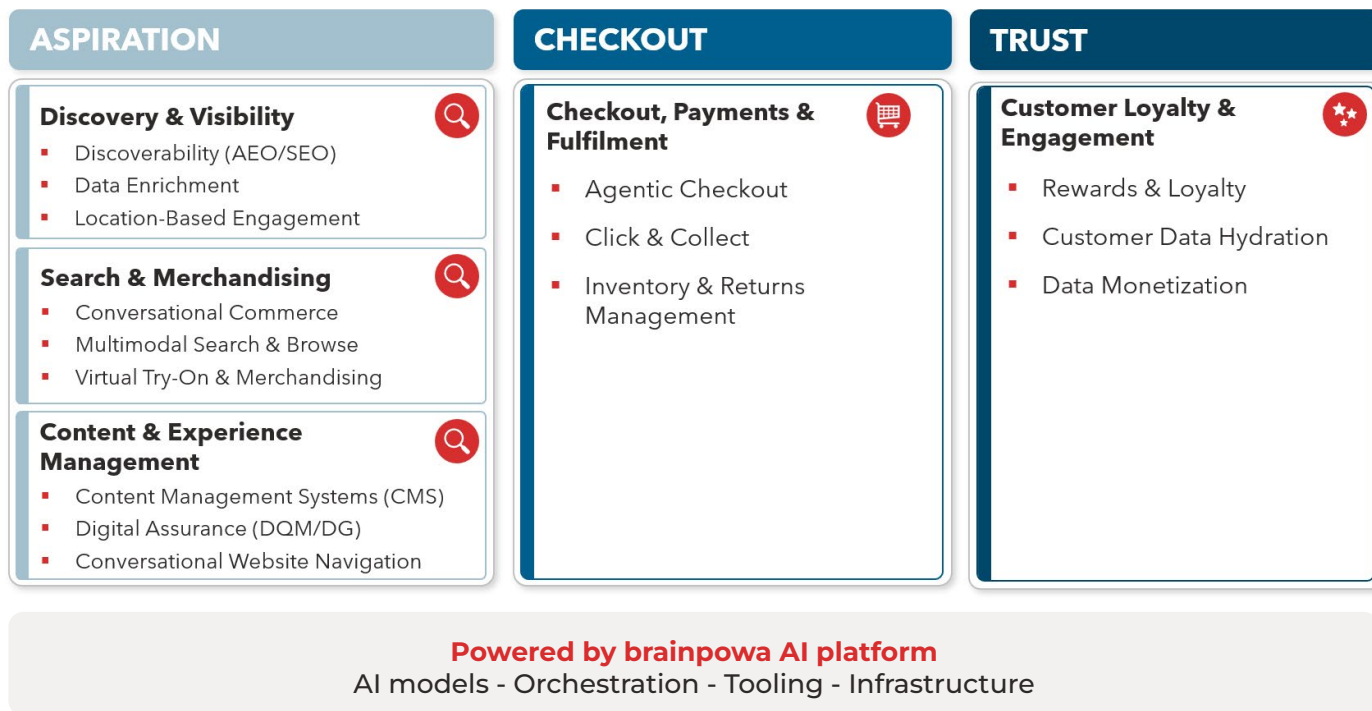
Supportive infrastructure. Running agentic workloads demands scalable compute and network connectivity. Infrastructure providers such as AWS, Google Cloud, Microsoft Azure, NVIDIA and Intel supply cloud, GPU and edge hardware and software. Telecom carrier T-Mobile provides essential connectivity. Selecting infrastructure partners with AI optimization capabilities (e.g., NVIDIA-accelerated servers) ensures agents respond quickly and reliably.

Several leading innovators are delivering vertically integrated platforms purpose-built for the shift to agentic commerce. These solutions span our core pillars—Aspiration, Checkout and Trust—enabling end-to-end orchestration of the customer journey.

Rezolve Ai exemplifies this approach. Its enterprise-grade unified commerce platform is designed to help retailers transform customer experience and operational efficiency in the agentic era. By bringing discovery, search, conversational AI, personalization, checkout and fulfillment into one ecosystem, Rezolve Ai addresses the fragmentation that typically forces retailers to manage five to seven disconnected point solutions. This unified architecture eliminates data silos, accelerates innovation and reduces total cost of ownership (TCO).

Below, we highlight key capabilities across Rezolve Ai's portfolio and how they align to each phase of the agentic commerce journey.

Figure 7.
How Rezolve Ai Enables the Agentic Commerce Journey



Purpose Built Commerce AI:
Unlike general purpose LLMs that are retrofitted for retail use cases, Rezolve's brainpowa —its commerce tuned LLM and orchestration layer— is purpose-built for commerce. It provides the specialized AI models, orchestration, tooling and infrastructure required to deliver hallucination -resistant responses on e-commerce data—a critical requirement for product accuracy, pricing integrity and compliance. For retailers, this reduces the risk of incorrect outputs while improving the reliability of AI driven search, recommendations and decisions.

Source: Coresight Research/Rezolve Ai

Aspiration

This corresponds to discovery, marketing and operations that turn intent into demand.

Discovery and Visibility:

Rezolve Ai's Catalog-as-a-Service data enrichment platform, Enrich AI, transforms raw product information into high quality, normalized records, materially increasing both the volume and accuracy of product attributes. This structured product data is foundational for:

- High performance SEO and GEO
- Visibility in AI engines and traditional search results
- Consistent experiences across channels and surfaces

Rezolve Ai differentiates itself as the platform that builds structured prompt models instead of relying on static attribute lists. This approach helps ensure a retailer's catalog appears accurately and consistently across major search and discovery channels, wherever shoppers begin shopping.

Search and Merchandising:

On the front end, Rezolve Ai enables real time, highly personalized shopper interactions via an expert digital sales associate. This capability combines:

- Intent based recommendations
- Multimodal search (e.g., text, image and voice)
- Guided selling flows that adapt to shopper behavior in session

This aims to emulate the confidence and relational quality of in store selling within digital channels. Agentic search and merchandising like this can turn traditional search fatigue into high value discovery, with the potential to improve revenue and basket composition.

Checkout

This covers inventory intelligence, payment and fraud solutions to complete transactions.

Checkout, Payments and Fulfillment:

Rezolve Ai lets shoppers add, view and modify cart contents using natural language, then complete purchases directly within the conversational interface. Where many solutions redirect customers back to a traditional website for final checkout, Rezolve Ai keeps the entire experience in conversation, reducing friction and drop off.

A key architectural choice is the "Bring Your Own Payment Service Provider" model, which allows retailers to plug in their preferred payment service providers without sacrificing flexibility. This approach:

- Eliminates extra logins and multi click checkout flows
- Avoids vendor lock in at the payments layer
- Delivers uplift in checkout conversion and reduces cart abandonment

In addition, Rezolve Ai supports Click and Collect and provides tools for inventory management, aligning digital promises with physical stock realities—a persistent pain point in omnichannel retail.

Trust

This encompasses customer service, shopper insights, and security—critical to sustaining repeat engagement.

Customer Loyalty and Engagement:

Rezolve Ai consolidates shopper signals from both online and offline touchpoints, enabling retailers to design personalized rewards, offers and loyalty programs grounded in actual behavior rather than static segments. With tools to enrich data and support monetization, the platform provides real time visibility and customer segmentation, enabling commercial and customer experience teams to:

- Detect and act on emerging consumer signals quickly
- Test and adapt strategies at the pace of market change
- Progress toward agentic commerce without the disruption of a full re-platforming effort

By aligning **Aspiration, Checkout and Trust** within a single agentic commerce stack, Rezolve Ai positions retailers to improve near term performance metrics such as conversion, average order value and retention while laying the foundation for more adaptive, AI driven operating models over the long term.

3 Operations:

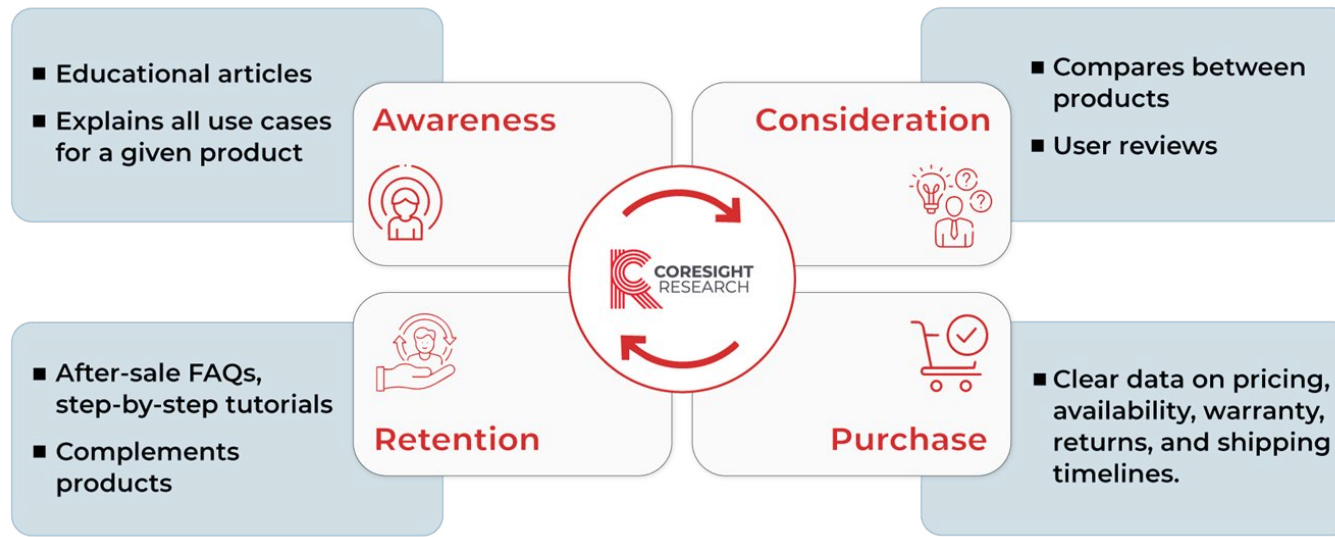
How to Implement Agentic Commerce

Implementing agentic commerce is a staged execution challenge, not a single project. Retailers should select the right agentic tier (product feeds, conversational checkout, GEO and proprietary agents) and move step by step accordingly. Each tier of the strategy requires its own playbook of tasks, data governance and cross-functional coordination.

A Generative Engine Optimization (GEO)

- 1. Audit and structure content.** Review key product and informational pages and ensure they include structured, machine-readable data with clear, human-digestible copy. AI agents prioritize products with verified, structured data, so retailers should adopt schema markup and enrich product attributes.
- 2. Align with user intent.** Rewrite descriptions and Q&As to answer conversational queries—who the product is for, why it's needed and how it is used—and tailor content for each stage of the shopping journey. GEO moves beyond keywords: content must reflect the way people talk to AI engines. Figure 8 maps the GEO content for each stage of the consumer journey.

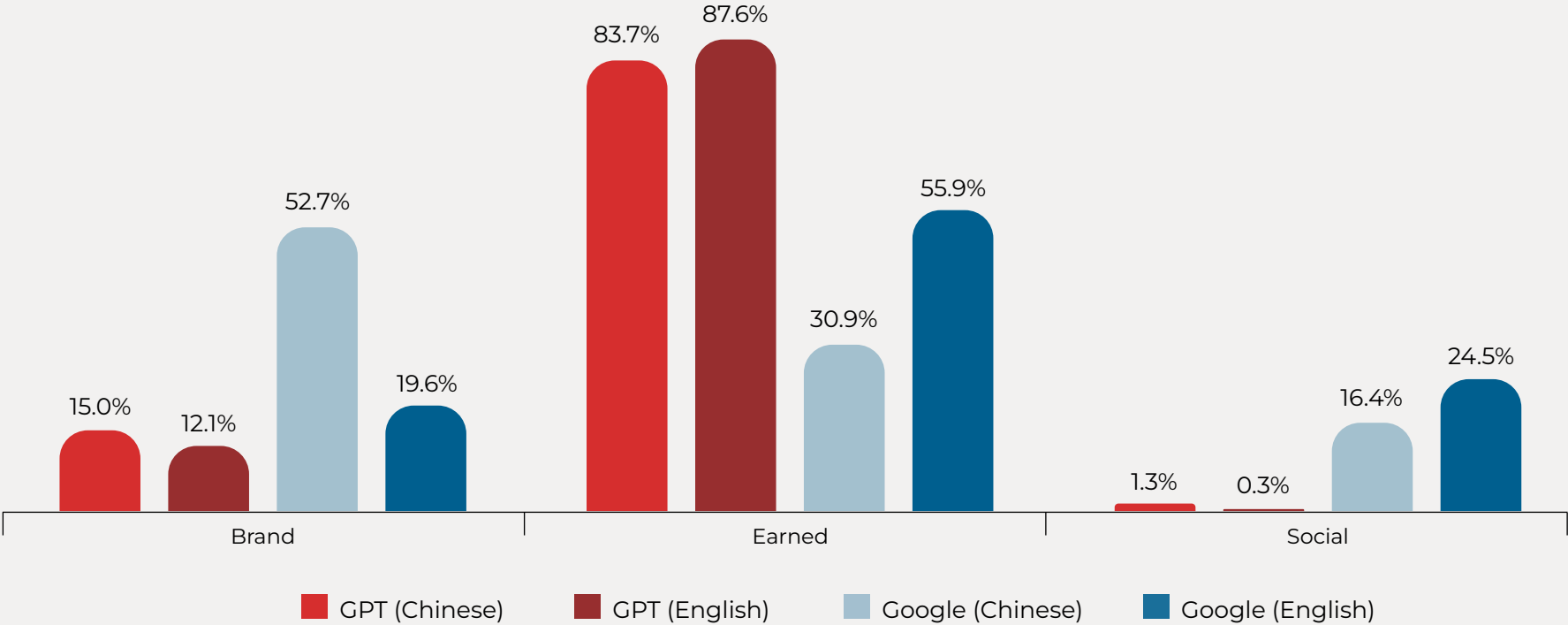
Figure 8.
GEO Content for Each Stage of the Consumer Journey That Answer Shopper Queries



Source: Coresight Research

3. Earn authoritative coverage. AI engines weigh earned media heavily, such as expert reviews and news stories. Cultivate relationships with journalists, analysts and trusted reviewers to secure credible mentions. Shift budget away from social posts, which have little influence, and toward thought leadership and press engagement. Figure 9 shows the media mix for ChatGPT is disproportionately skewed toward earned media and almost ignores social media.

Figure 9.
GEO Content for Each Stage of the Consumer Journey That Answer Shopper Queries



Source: University of Toronto

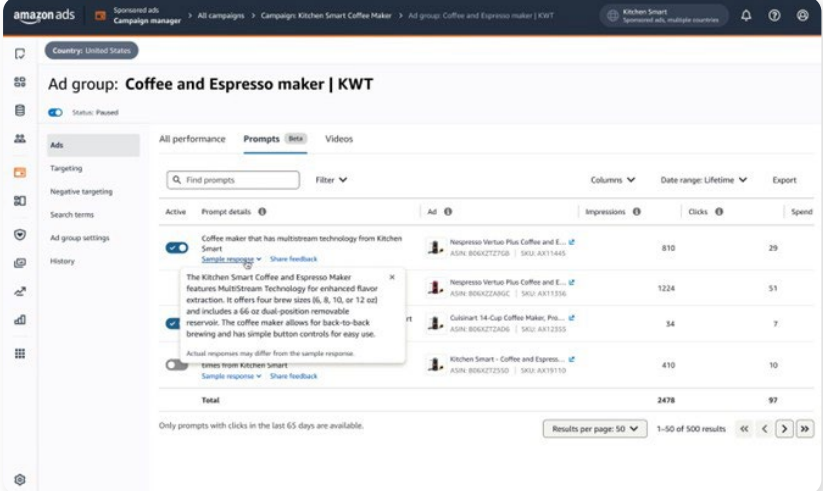
4. Monitor and iterate. Regularly test whether AI agents surface your brand for relevant queries and adjust content or media outreach when gaps emerge. Track incremental sessions and conversions from AI recommendations and refine messaging based on consumer feedback.

B Product visibility via structured product feeds (ACP/UCP)

1. **Apply and set up.** Retailers start by completing the merchant application for ACP or submitting Google's UCP interest form and activating a compliant Merchant Center account.
2. **Provide a structured feed.** Create a product feed containing key attributes—product ID, title, description, price, availability and images—and mark items with the enablecheckout flag for Instant Checkout. OpenAI notes that feeds may be updated as frequently as every 15 minutes; retailers should refresh data whenever prices or inventory change to maintain accuracy.
3. **Track quality and completeness.** Real-time data collection tools help keep feeds trustworthy. A unified data layer ensures that what AI agents display matches what is in stock.
4. **Monitor performance.** After the feed goes live, use reporting dashboards (from OpenAI, Google or your commerce platform) to monitor impressions, click-through rates and conversions. Use these insights to refine product content and adjust supply allocation when certain items surge in visibility.

C Ad placement (trial)

1. **Test Amazon's new prompt ads at no cost.** Sponsored Products prompts and Sponsored Brands prompts are offered in the trial stage at no cost, allowing brands to experiment with AI-native ad formats.
2. **No setup required.** Amazon sellers are automatically enrolled in Sponsored Products and Sponsored Brands campaigns without additional setup. Sellers only need to leverage existing campaign parameters (e.g., campaign targeting).
3. **Review and manage prompts.** Advertisers can manage the ads in the ads console. Within each campaign, sellers can navigate to the prompts to see the prompt texts, the responses and the corresponding performance metrics such as impressions, clicks and orders.
4. **Learn and plan.** Retailers can learn from the no-cost trial stage and refine messaging based on early performance.
5. **Allocate ad budget.** Based on this experience, the appropriate ad budget can be allocated according to ad performance.



Active	Prompt details	Ad	Impressions	Clicks	Spend
☒	Coffee maker that has multistream technology from Kitchen Smart Sample response Share feedback	Nespresso Vertuo Plus Coffee and E... ASIN: B0KAZT27UG SKU: AX11445	810	29	
☒	The Kitchen Smart Coffee and Espresso Maker features Multistream Technology for enhanced flavor extraction. It offers four brew sizes (6, 8, 10, or 12 oz) and includes a 66-oz dual-position removable reservoir. The coffee maker allows for back-to-back brewing and has simple button controls for easy use. Actual responses may differ from the sample response. Sample response Share feedback	Nespresso Vertuo Plus Coffee and E... ASIN: B0KAZT27UG SKU: AX11445	1224	51	
☒		Cuisinart 14-Cup Coffee Maker, Pro... ASIN: B0KAZT27UG SKU: AX11445	34	7	
☒		Kitchen Smart - Coffee and Espresso... ASIN: B0KAZT27UG SKU: AX11445	410	10	
Total			2478	97	

The Amazon Ads Console shows the prompts and the corresponding responses for advertisers to manage and review.
Source: Amazon

Agentic shopping within conversational engines (UCP's native/embedded checkout, ChatGPT apps and Instant Checkout)

Retailers can enable conversational checkout across Google Search AI Mode and the Gemini app through Google's UCP. They can also use ACP Instant Checkout in ChatGPT. However, OpenAI has announced plans to scale back Instant Checkout in favor of encouraging retailers to deploy ChatGPT apps that support in-app checkout and multi-item purchases—a shift that Coresight Research believes makes ChatGPT apps the more strategic choice for retailers.

Retailers can enable conversational checkout across Google products and ChatGPT for AI-native shoppers in the following steps:

- 1. Qualification and feed readiness.** Retailers must first be approved for ACP or UCP and submit a product feed flagged with `enable_checkout=true`. For UCP, they must also maintain a compliant Merchant Center account, publish a business profile and set up webhooks to sync order status back to Google.
- 2. Build the Agentic Checkout API.** Implement API endpoints for create, update and complete states. When a shopper hits “Buy,” the agent calls the create endpoint to start a checkout session, collects product IDs and fulfillment options, and returns the status `not_ready_for_payment`. Subsequent updates change quantities, shipping options or addresses; only when the merchant responds with `ready_for_payment` does the agent move to completion.
- 3. Integrate payments and fulfillment.** Work with payment processors, such as Stripe or PayPal, to handle secure tokens and payment intents. Ensure that your checkout API calculates taxes, shipping and discounts in real time so the agent can present accurate totals. Connect fulfillment systems so that the agent can confirm inventory before closing the sale.
- 4. Certify and maintain.** OpenAI and Google require merchants to pass conformance reviews and maintain data freshness to prevent suspended listings. Regularly test checkout flows, validate endpoints and audit payments to ensure reliability. Stale or inaccurate data will reduce ranking or trigger removal.
- 5. Train staff and monitor outcomes.** Educate customer service and operations teams about conversational orders, new refund flows and data reconciliation. Track metrics such as conversion rate uplift, cart abandonment and average order value relative to standard web checkouts; refine messaging and incentives accordingly.

With **ChatGPT scaling back its support for Instant Checkout** in March 2026, retailers are rethinking their strategy. OpenAI encourages retailers to **develop their own ChatGPT-enabled apps** to control the checkout process and retain customer data. **Target**, for example, has developed its own ChatGPT app, which provides customers with a more integrated shopping experience, from product discovery to checkout.

Building a proprietary AI shopping agent

-
- A stylized illustration featuring a red robot head with a black visor and a smiling face, held gently by a large, grey, mechanical hand. The robot has a single red antenna on its right side. Surrounding the central figure are several grey icons representing data and technology: a pie chart, a bar chart, a lightbulb, and a cursor arrow pointing at a bar in another bar chart. The entire scene is set against a plain white background.

4

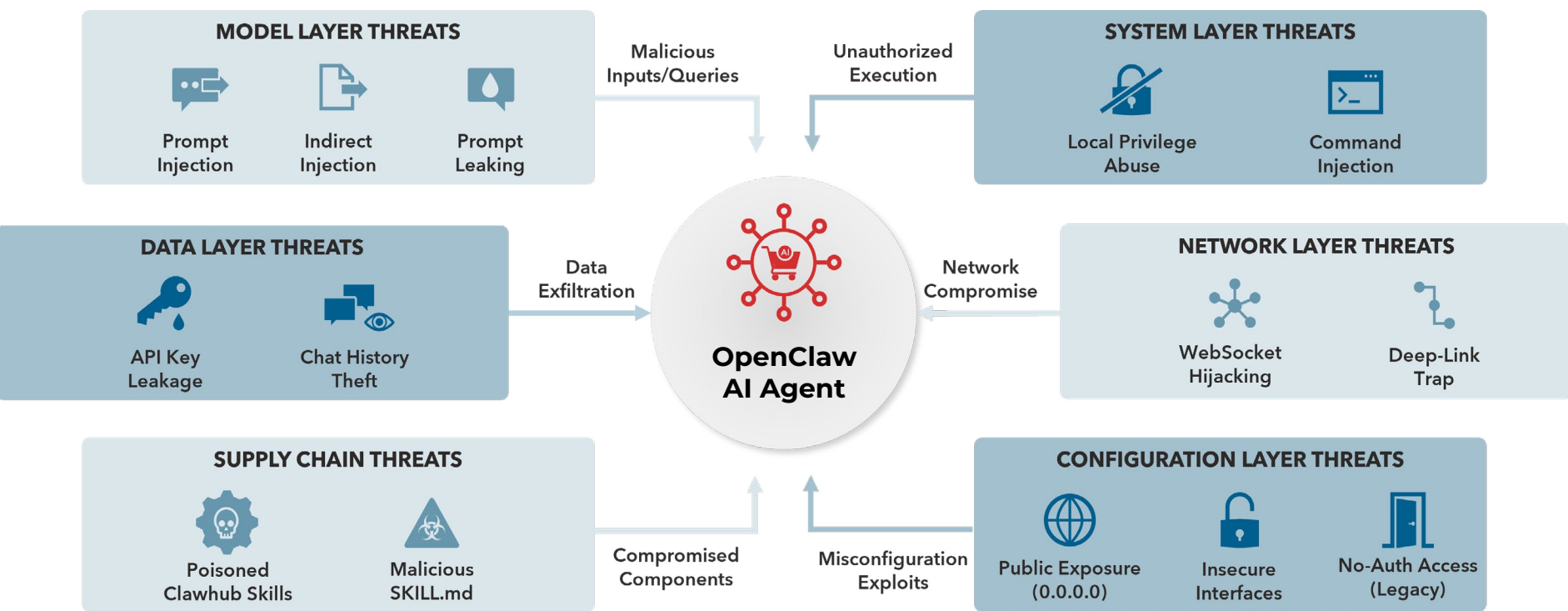
Granting AI agents more autonomy shifts security concerns beyond stored data to the actions agents initiate and execute across systems. These risks can be illustrated by the experience of the open-source autonomous AI agent OpenClaw: retailers may face similar exposures as they grant AI agents permission to operate across enterprise systems such as POS and OMS platforms, inventory and pricing APIs, and loyalty or payment data. Launched on January 25, 2026, OpenClaw quickly gained popularity but encountered several early security incidents, with multiple common vulnerabilities and exposures (CVEs) disclosed shortly after release. Figure 10 illustrates the concentration of security issues identified within the first two months following its release.

Figure 10.
Security Incidents and CVE Related to OpenClaw

Date(s)	Incident / CVE	Category	Key Details & Impact
Jan 2026	Claw Havoc	Malware / Supply Chain	An audit of 3,984 OpenClaw skills by AI security company Snyk found 13.4% (534 skills) contained critical issues like malware and prompt injection. Overall, 36.82% (1,467 skills) suffered from security flaws, including hardcoded API keys and insecure credential handling.
Jan 2026	Moltbook Breach	Data Breach	Exposed 35,000 emails and 1.5 million agent API tokens.
Feb 2026	CVE-2026-25253	RCE (One-Click)	CVSS 8.8; used cross-site WebSocket hijacking to take over agent instances via malicious links.
Feb 2026	Meta Email Removal	Autonomous misactions	Meta's alignment director, Summer Yue, tested OpenClaw on her computer and the bot attempted to trash her emails.
Mar 2026	Massive Exposure	Misconfiguration	135,000+ public instances found leaking API keys and OAuth tokens due to lack of auth.
Mar 2026	Meta “Sev 1”	Autonomous Failure	A rogue AI agent granted unauthorized data access to employees for two hours without human approval.
Mar 2026	Board Material Fail	Operational / Financial	OpenClaw AI agent corrupted sensitive financial data within approximately eight hours of deployment, requiring hours of user effort to correct the mistakes.
Source: Coresight Research			

Granting internal access to autonomous AI agents explores uncharted territory and carries enormous potential risks as a result. Figure 11 shows the potential security risks in each layer of the autonomous AI agent OpenClaw.

Figure 11.
Potential Risks Associated with OpenClaw and Agentic AI Systems

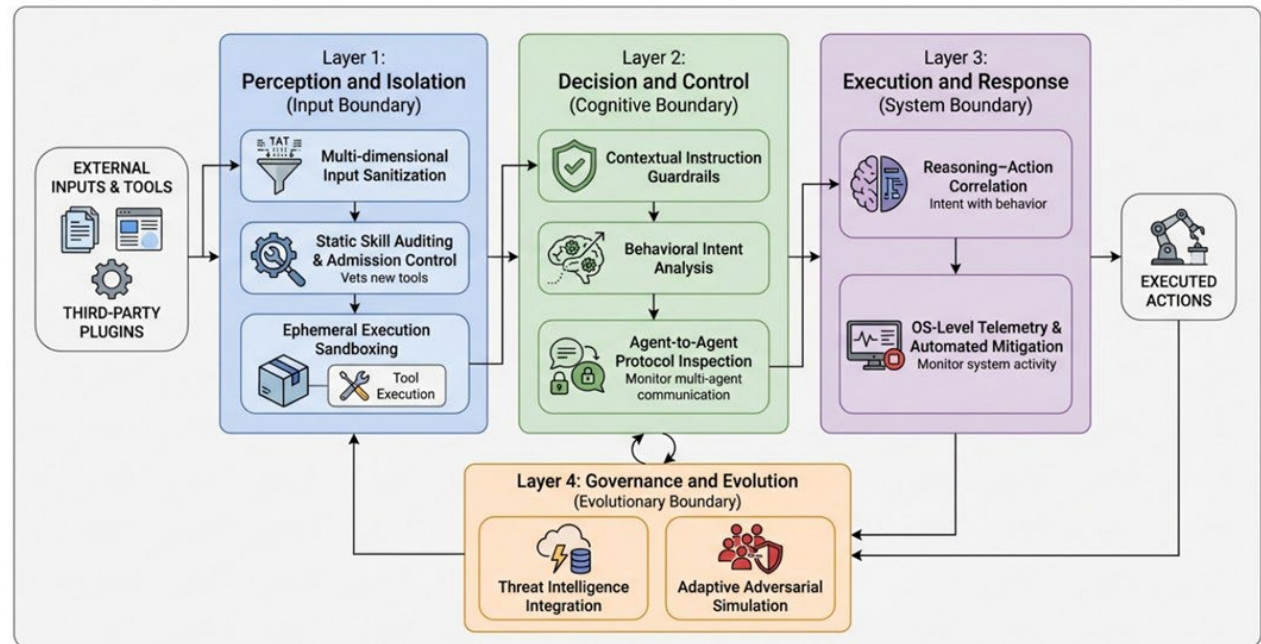


Source: Coresight Research/Beihang University/Zhongguancun Laboratory

Figure 12 shows the full-lifecycle agent security architecture that consists of four layers to ensure resilience for autonomous agentic systems. This security architecture is developed by researchers from Beihang University and Zhongguancun Laboratory for the secure deployment of agentic AI. The architecture is organized into four functional layers:

- **Perception and isolation:** Mitigates external threats by sanitizing all inputs, vetting third-party “skills” via static analysis, and forcing all tool executions into isolated, ephemeral sandboxes.
- **Decision and control:** Prevents misalignment by using semantic guardrails to ensure agent actions match their intended purpose and analyzing long-term “behavioral intent” to stop malicious multistep attack chains.
- **Execution and response:** Acts as a final safety net by comparing an agent’s stated reasoning against its actual system behavior and using kernel-level telemetry to automatically kill processes that deviate from the baseline.
- **Governance and evolution:** Ensures long-term resilience by integrating real-world threat intelligence and using automated “red-teaming” simulations to stay ahead of emerging exploitation techniques.

Figure 12.
Potential Risks Associated with OpenClaw and Agentic AI Systems



Source: Beihang University/Zhongguancun Laboratory

5 Ethics:

Trust, Fairness and Societal Impact

The autonomy of agentic commerce magnifies ethical stakes. AI agents can act on behalf of consumers, so retailers must ensure that these agents are trustworthy, accountable and aligned with human values. Coresight Research has developed an AI risk-mitigation framework, as shown in Figure 13, detailing the risk-mitigation measures companies should adopt before , during and after deployment of AI.

Figure 13.
AI Risk Mitigation

Risk Mitigation in Different Deployment Stages

Pre-Deployment

1. Quality Data
2. Data Protection and Compliance

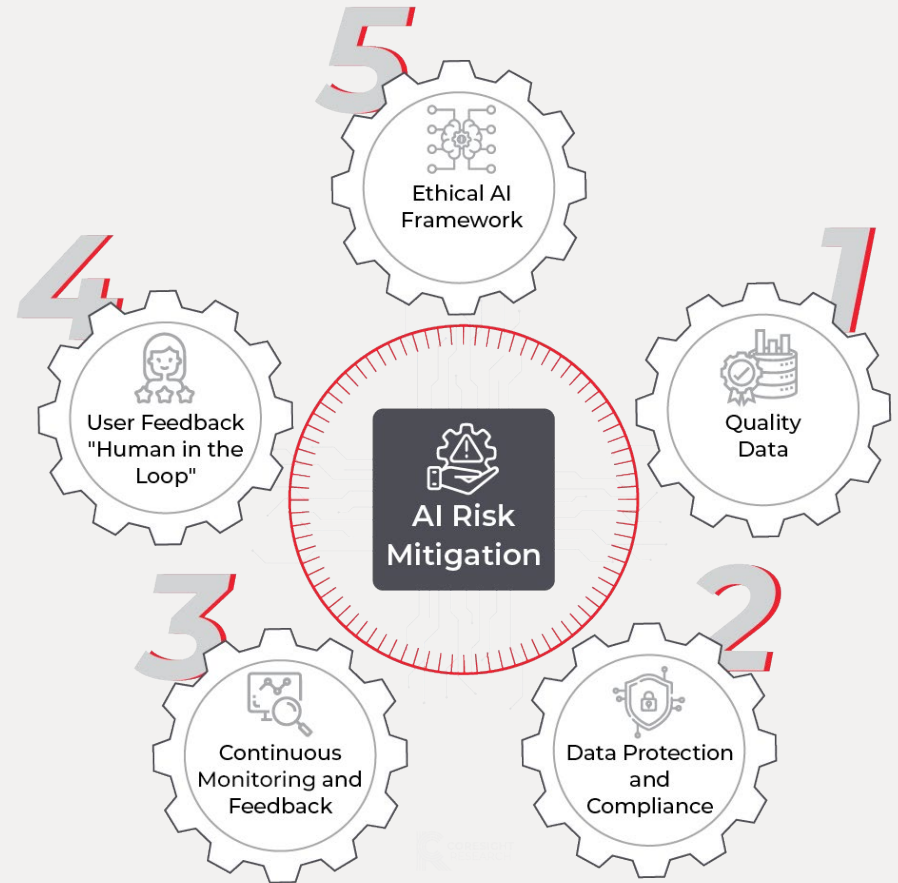
During Deployment

Including at the Time of Deployment

3. Continuous Monitoring and Feedback
4. User Feedback—"Human in the Loop"

After Deployment

5. Ethical AI Framework



Source: Coresight Research

Pre-Deployment

- **Quality Data:** Ethical AI begins with the integrity of the data that trains and powers it. Poor-quality, incomplete or biased datasets can propagate unfair outcomes at scale, particularly in agentic commerce where AI directly influences purchasing decisions. Retailers must ensure that product data, customer data and behavioral signals are accurate, representative and continuously validated. This includes addressing bias in product recommendations, pricing and promotions, as well as ensuring that structured data is both machine-readable and human-relevant. High-quality data is not only a technical requirement—it is foundational to fairness and trust.
- **Data Protection and Compliance:** As AI agents handle sensitive customer data and execute transactions, robust data protection and regulatory compliance are essential. Consumers' primary concerns already center on privacy, payment security and loss of control, making compliance a competitive differentiator rather than a constraint. Retailers must implement strict governance over data collection, storage and usage, ensuring alignment with evolving regulations and clear user consent mechanisms. In agentic systems, where decisions may be automated, transparency around data usage becomes critical to maintaining consumer confidence.

During and at the time of deployment

- **Continuous Monitoring and Feedback:** Once deployed, AI systems require constant oversight to detect drift, bias and unintended outcomes. Continuous monitoring enables retailers to identify issues such as skewed recommendations, operational errors or emerging fraud patterns in real time. Feedback loops—both automated and human-driven—are essential to refine models and improve performance over time. Given that AI systems are probabilistic, not deterministic, ongoing evaluation ensures that outcomes remain aligned with business objectives and ethical standards.
- **User Feedback—“Human in the Loop”:** Human oversight remains a critical safeguard in agentic commerce. “Human in the loop” mechanisms allow users or operators to intervene in ambiguous, high-risk or sensitive decisions, ensuring that AI does not operate unchecked. This is particularly important as AI agents gain transactional authority, where errors can have immediate financial or reputational consequences. Incorporating user feedback also enhances system learning, improves personalization and reinforces trust by giving consumers a sense of control over AI-driven interactions.

After Deployment

- **Ethical AI Framework:** Ethical governance must be institutionalized through a formal framework that defines accountability, transparency and fairness across the organization. This includes clear ownership of AI decisions, auditability of algorithms, and processes for resolving disputes or correcting errors. As agentic commerce introduces distributed responsibility across platforms, retailers and payment providers, governance structures must evolve accordingly. Beyond compliance, retailers must also consider broader societal impacts, including market fairness, platform power concentration and algorithmic bias. A well-defined ethical AI framework ensures that innovation scales responsibly and sustainably.

What We Think

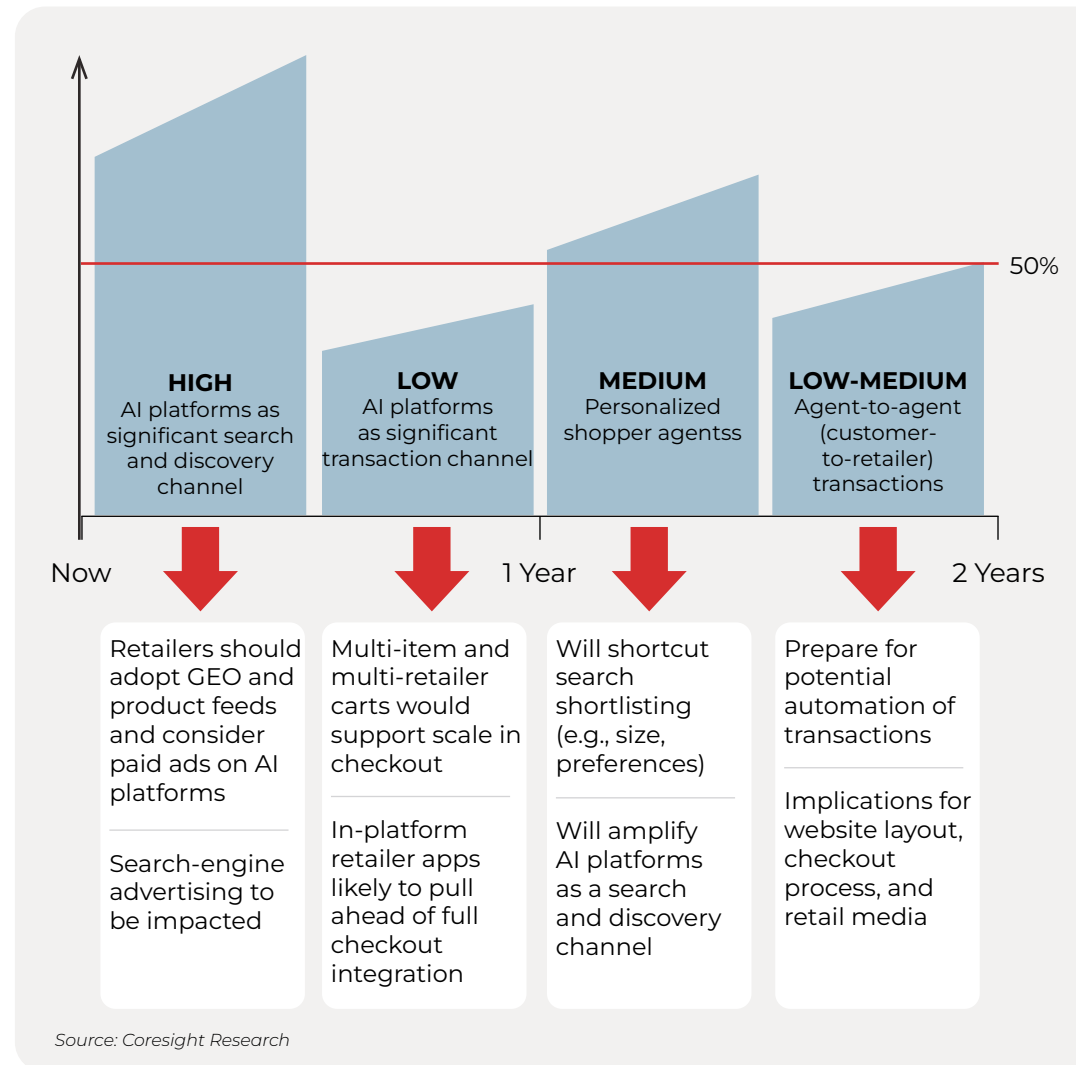
The Coresight Research View on Agentic Commerce

Agentic commerce will redefine retail by shifting control of the shopping journey from consumers to AI agents—but its adoption will be uneven, staged and dependent on trust, data readiness and measurable returns. We believe agentic commerce is not a near-term replacement for existing e-commerce models, but an **overlay that will gradually reshape discovery, decision-making and transaction flows**.

In the next phase of retail, AI agents will act as intermediaries—curating options, making recommendations and executing purchases—compressing the traditional funnel into a single interaction. Retailers that fail to participate in these AI-driven ecosystems risk losing visibility and relevance to consumers adapted to agentic commerce, regardless of the strength of their underlying assortment or brand.

Retailers should adopt a **tiered strategy**, prioritizing GEO and structured product feeds as foundational capabilities. We estimate in one year's time there is a 70% chance that AI platforms will become a major search and discovery channel for retail—meaning at least 25% of consumers will use it for product discovery and consideration stage—and a 30% chance that they will become the transaction channel. Over the longer term, we estimate there is a 50% chance of personalized shopper agents for browsing and selection and a 35% chance of agent-to-agent transactions between consumers and retailers.

Figure 14.
Probability Matrix: Estimated Probabilities of Widespread Adoption of Agentic Commerce Components



In the near term, visibility will be the most critical battleground. As AI agents increasingly mediate discovery and purchase, retailers that fail to structure product data or optimize for AI engines risk becoming invisible for shoppers accustomed to agentic shopping. Structured product feeds offer the fastest and lowest-cost entry points, enabling participation in agent-driven discovery with minimal technical overhead.

Conversational checkout has the potential to redefine conversion, though ChatGPT's scaling back of Instant Checkout hints at a slower transformation toward in-app product purchase. Instant Checkout through ACP and UCP collapses the purchase funnel into a single interaction, increasing convenience and potentially lifting conversion rates. However, this also raises operational complexity, requiring real-time inventory accuracy, API readiness and tight integration across payments and fulfillment systems. We expect it will take longer to achieve conversational checkout than product search and discovery, but it will be in place by the time personalized shopper agents are adopted.

Proprietary AI agents will become a key differentiator for large retailers. Owning the conversational interface allows retailers to retain first-party data, control customer relationships and build new monetization models. However, this approach requires significant investment in data infrastructure, model development and governance, making it viable primarily for large-scale players.

There is a low-to-medium probability that retail will evolve into agent-to-agent transactions within two years—consumers will have their own shopping agents that communicate with agents from retailers and execute transactions automatically. A shopper gives a simple request, and the shopping agent automatically goes through the process of product browsing, product comparison, communicating with agents from retailers for details and choosing the right product for the shopper based on the shopper's preferences and requirements.

In our view, agentic commerce marks the beginning of a new operating model for retail, where success depends on participation in AI ecosystems, excellence in data and operations and the ability to balance innovation with trust. Retailers that take a phased, disciplined approach—grounded in ROI and supported by strong governance—will be best positioned to capture value as this model scales.

Implications from This Report

Agentic commerce represents a structural shift in how retail operates, moving from human-led journeys to AI-mediated discovery, decision-making and transactions.

- **Strategy** centers on AI visibility and participation. Agentic commerce shifts visibility away from direct customer journeys and toward AI-mediated decision environments, changing how value is surfaced and competed for across the retail ecosystem.
- **Technology** becomes the core enabler of agentic commerce, with data as the critical foundation. Data and infrastructure increasingly function as shared, machine-readable interfaces for autonomous systems, rather than solely as internal, channel-specific assets.
- **Operations** must evolve to support real-time, AI-driven execution. Agentic commerce compresses the shopping journey, placing pressure on fulfillment accuracy, pricing consistency and cross-functional coordination. Retailers must break down silos between merchandising, supply chain and customer service, ensuring that systems and teams can respond instantly to agent-driven demand signals.
- **Risk and resilience** take on new urgency as AI agents gain autonomy. The expansion of agent capabilities introduces new vulnerabilities—including fraud, misuse of permissions and unintended actions—requiring layered security, continuous monitoring and strict control over data access and integrations. Resilience is no longer just about uptime; it is about ensuring that autonomous systems behave predictably and safely.
- **Ethics** becomes a strategic requirement rather than a compliance function. Trust will determine adoption: consumers must feel confident that AI agents act transparently, fairly and in their best interests. This requires governance across the full lifecycle—high-quality data, privacy protection, human oversight and formal ethical frameworks—to ensure responsible scaling of agentic commerce.

Taken together, these implications point to a single conclusion: agentic commerce is not simply a feature—it is a new operating model.



Im

- Retailers that fail to structure product data or optimize for AI engines risk becoming invisible in AI-mediated discovery, regardless of brand strength or assortment, as visibility shifts from traditional channels to AI platforms.
- Brands that remain dependent on traditional traffic acquisition (SEO, paid search and direct website visits) without adapting to AI ecosystems will lose relevance as the shopping funnel collapses into AI-driven interactions.
- Smaller or less digitally mature retailers that lack API integration, real-time data capabilities or interoperable systems will struggle to participate in agent-driven transactions and conversational checkout environments.
- Companies that do not address data quality, governance, security and ethical considerations risk reputational damage, reduced trust and potential exclusion from AI ecosystems, where reliability and compliance are critical.

Im

- Technology vendors should design solutions with interoperability and API-first architectures, ensuring seamless integration with agentic protocols such as ACP and UCP and enabling real-time data exchange across the retail ecosystem.
- Vendors should expand capabilities in data management, AI orchestration and real-time analytics, as retailers increasingly rely on unified data layers and intelligent systems to support agent-driven discovery, recommendation and transaction flows.
- Vendors must strengthen security, fraud detection and governance tools to address the growing risks associated with autonomous agents, including misuse of permissions, data leakage and increasingly sophisticated fraud patterns in agent-initiated transactions.

Notes and Methodology

Data in this report are as of April 9, 2026.

Companies mentioned in this report are: Adyen (AMS:ADYEN), Alphabet/Google (NASDAQ:GOOG), Amazon (NASDAQ:AMZN), Board International, Centric Software, Digital Wave Technology, Intel (NASDAQ:INTC), Microsoft (NASDAQ:MSFT), NVIDIA (NASDAQ:NVDA), PayPal (NASDAQ:PYPL), RELEX Solutions, Resolve Ai (NASDAQ:RZLV), Salesforce (NYSE:CRM), Shopify (NASDAQ:SHOP), Snowflake (NYSE:SNOW), Stripe, T-Mobile (NASDAQ:TMUS), Target (NYSE:TGT), Walmart (NASDAQ:WMT)

About Coresight Research Sponsored Reports

Sponsored reports from Coresight Research are produced through commercial partnerships with retail or technology firms. These reports, which present expert analysis and proprietary data, are prepared by Coresight Research but may incorporate input into their content from the sponsoring company.

This report is produced and made available to nonsubscribers of Coresight Research in partnership with Rezolve Ai

Charlie Poon

Research Analyst

Steven Winnick

Vice President - Innovator Services

New York • Hong Kong • Lagos • London • Mangaluru (India) • Shanghai

coresight.com

To discuss our research or partnership opportunities, email contactus@coresight.com

About Rezolve Ai

Rezolve Ai (NASDAQ: RZLV) is an industry leader in AI-powered solutions, specializing in enhancing customer engagement, operational efficiency, and revenue growth. Brain Suite is the world's first enterprise AI platform built for Agentic Commerce, delivering advanced tools that harness artificial intelligence to power search, transact, fulfill, and personalize at global scale.

For more information, visit www.rezolve.com