DATASHEET

strivacity

Strivacity for Agentic Commerce

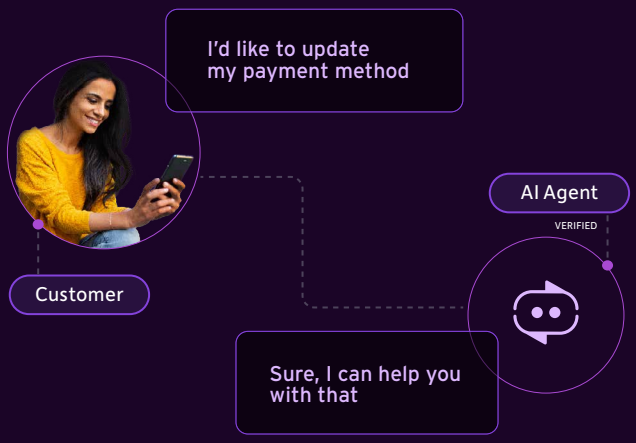
BUILT FOR AGENTIC COMMERCE

By 2028, 90% of B2B buying will be intermediated by AI agents.[1] They're already inside your digital experiences, signing in, requesting data, comparing options, and making recommendations. But unlike most agentic use cases outside of commerce, they aren't yet taking actions. Whether it's completing purchases, transferring balances or sending purchase orders (among countless others), agentic transactions aren't yet widespread.

The problem: the safeguards and controls necessary for trustworthy agentic commerce are missing. Which agents should be allowed to request access to my customers' accounts? What limits on transactions should I enable to put my customers in control? How can I stop agentic fraud?

Strivacity is building the answer: one product that governs AI agents, customers, and partners using the same policy engine, with MCP authorization, agentic trust intelligence, and a unified audit trail that makes delegation transparent. All of the benefits of Strivacity, extended to cover agentic commerce.

[1] *Gartner Unveils Top Predictions for IT Organizations and Users in 2026 and Beyond*



> "Strivacity gave us a secure, modern online experience for our customers while saving us $2M vs what we spent with Okta and Ping Identity."
>
> — CISO, Top 20 US Bank

Benefits

1 Verification of who the agent is

Know the agents accessing your systems on behalf of customers. Strivacity analyzes agent trust signals and combines them with the same document verification and fraud signals used for your customers, before issuing any credential.

2 Visibility into what agents did

Without agentic identity, customer and agent actions look identical in your logs. The Strivacity Dashboard provides a unified log of human and agent activity, turning it into insights you can act on and evidence you can present to regulators.

3 Control over what agents can do

Agents act only within fine-grained, customer-granted permissions. Customers control what each agent can do, and revoke access instantly through their account portal.

Built for every stakeholder in your buying committee

CISO

Unified audit trail across every human and AI agent interaction. Adaptive access and fraud controls actively block threats. Identity data stays exactly where you place it, by design.

CTO / VP ENGINEERING

Pre-built components, SDKs, and APIs let your team focus on the product. Configure in Journey Builder, extend with code. No re-platforming as your agentic use cases grow.

VP PRODUCT & DIGITAL

Real-time visibility into where AI agent flows affect conversion. Built-in A/B testing and low-code controls let you optimize customer journeys fast.

COMPLIANCE & LEGAL

Versioned, auditable consent records for every agent permission. Support for GDPR, EU AI Act accountability requirements, and your preferred data residency region. No surcharge.

VP PAYMENTS / FRAUD & RISK

Fewer legitimate agents flagged as fraud. Fewer bots waved through as real customers, thanks to document verification and fraud signals applied before any credential is issued.

©2026 Strivacity. All rights reserved.

How it works

Secure delegation for AI agents
AI agents need authority to act. In agentic commerce, that authority often involves money, and therefore must be explicit, not implied. Customers authorize agents via explicitly scoped permissions, building their trust in agentic commerce by putting them in control. Strivacity implements delegation semantics to authorize access to MCP servers. Delegation is bound to consent and stored as an auditable record.

Unified audit trail & insights
Every agent action is captured in the same audit trail as human activity, attributed to both the agent and the authorizing person. Dashboard insights surface agent-driven patterns, conversion data, and risk signals, creating a chain of custody suitable for regulatory review.

AI data residency
Agentic identity data is stored and processed within customers' chosen regions to meet local regulatory and privacy requirements.

Agent access policies
Set policies on which agents are allowed to request access to your customers' accounts, based on where they originate. Create adaptive authentication policies which vary authentication requirements for agent authorization.

Policy-driven journey execution
The agent executes within boundaries defined in Journey Builder. Risk-based decisioning, adaptive MFA, and real-time fraud signals govern every step, applying the same controls as human sign-in.

My agents self-service
Your customers see every agent on their account: what it can do, what it has done, and how to revoke access. All in one place, without contacting support. Because trust should be revocable.

NAMED A CIAM LEADER

Forrester Wave™: Customer Identity and Access Management Solutions, Q4 2024 gave Strivacity the highest possible score in 12 criteria, more than any other vendor evaluated.

"Customers praised the Strivacity responsive support and engineering, and low-code/no-code orchestration and customer self-service built-in capabilities are easy to use."

Platform capabilities supporting agentic commerce

Identity orchestration
Governs agent behavior in Journey Builder, Strivacity's low-code orchestration tool. Defines the exact sequence of authentication, verification, consent, and approval steps required. No separate dev project.

Consent management
Captures customer consent and preferences, with auditable consent receipts.

Single-instance data residency
Keeps AI, customer, and partner identity data in your chosen region, isolated by architecture. No shared tenants, no surcharge.

Identity lifecycle management
Manages the full lifecycle of identities from registration to revocation.

Adaptive access for agents
Applies the same adaptive intelligence that protects your customers to govern AI agent behavior. Evaluates risk signals at every authorization decision, applies step-up authentication, and keeps automation within safe limits.

Self service account management
Enables customers to manage profile updates, credentials, and preferences through self-service. No support ticket required.

Built on standards
Built on OAuth 2.1, PAR, RAR, DPoP, ID-JAG, MCP, and CIBA.

AI assist:
Built-in AI assistant for setup, optimization, and troubleshooting across human and agent journeys.

