

Strivacity for Agentic AI



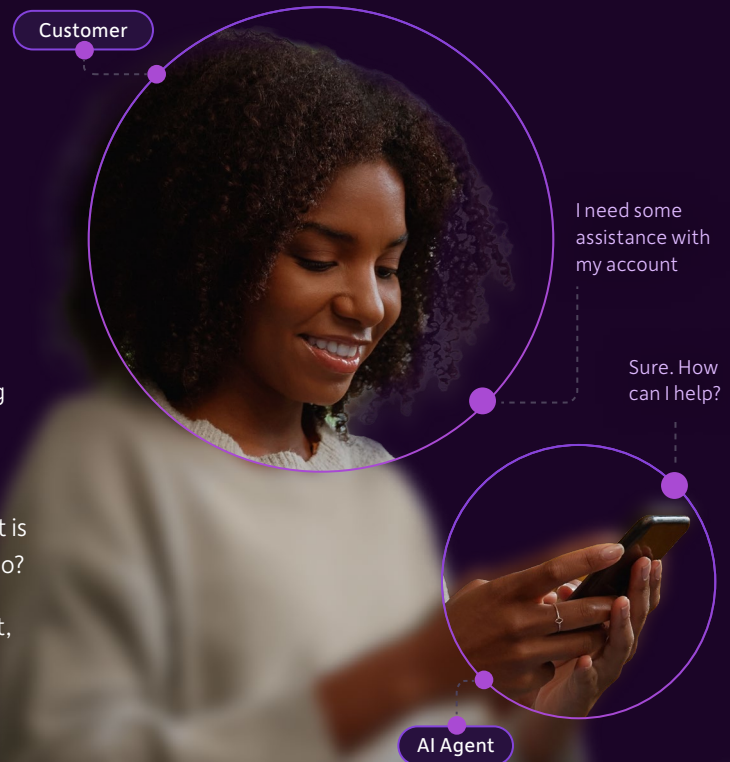
ONE PRODUCT FOR HUMANS AND AI AGENTS

By 2028, 90% of B2B buying will be intermediated by AI agents.¹ They're already inside your digital experiences, signing in, requesting data, and acting on behalf of real customers.

The problem: they're doing it with credentials built for humans. Traditional CIAM has no way to answer the questions that follow: What is this agent allowed to do? Who authorized it? And what did it actually do?

Strivacity governs AI agents, customers, and partners in one product, built on the same policy engine, with a unified audit trail and the administration experience you already use. All of the benefits of Strivacity, extended to cover AI.

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



Benefits

1

Verification of who the agent is

Know the agents accessing your systems. Strivacity works with agent trust frameworks 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 the My Agents 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.

How it works

- ▶ **Secure delegation for AI agents**
AI agents need authority to act. Customers authorize agents via explicitly scoped permissions. Strivacity implements delegation semantics to authorize access to MCP servers. Delegation is bound to consent and stored as a versioned, auditable record.
- ▶ **AI data residency**
AI identity data is stored and processed within customers' chosen regions to meet local regulatory and privacy requirements.
- ▶ **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.
- ▶ **MCP server**
AI agents can call Strivacity directly as an MCP server to retrieve identity context, check delegation scope, and trigger identity workflows. Agents are governed by the same policies as human interactions.
- ▶ **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.
- ▶ **Know your agent (KYA)**
When an organization-deployed agent requests access, Strivacity verifies the agent and the human or organization behind it via document verification and fraud signals before issuing any credential.
- ▶ **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 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.

”

Strivacity capabilities supporting agentic AI

- **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.
- **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, apply step-up authentication or require human approval, and keeps automation within safe limits.
- **Consent management**
Captures customer consent and preferences with versioning and auditable consent receipts.
- **Self service account management**
Enables customers to manage profile updates, credentials, and preferences through self service. No support ticket required.
- **Single-instance data residency**
Keeps AI, customer, and partner identity data in your chosen region, isolated by architecture. No shared tenants, no surcharge.
- **Built on standards**
Built on OAuth 2.1, PAR, RAR, DPoP, ID-JAG, MCP, and CIBA.
- **Identity lifecycle management**
Manages the full lifecycle of identities from registration to revocation.
- **AI assist**
Built-in AI assistant for setup, optimization, and troubleshooting across human and agent journeys.

