

E-Book

The omnichannel identity playbook: Does your customer feel known everywhere?



Table of Contents

1	Summary
3	The Recognition Gap — why omnichannel was always a backend problem
6	From Recognition Gap to Recognition Advantage
9	The Auth0 playbook — how identity becomes the growth engine
12	In practice: Customer results
15	Key takeaways

These materials are intended for general informational purposes only and are not intended to be legal, privacy, security, compliance, or business advice. You are responsible for obtaining security, privacy, compliance, or business advice from your own professional advisors.



Summary

According to [McKinsey's Omnichannel Compendium for Retailers](#), 64% of consumer brands call a defined cross-channel strategy their primary lever for growth. Yet, 78% of those same organizations admit they still have no single-brand experience across their digital and physical channels.

For a decade, business leaders have correctly diagnosed the goal—delivering a seamless, personalized experience wherever a customer shows up—while incorrectly diagnosing the obstacle. Omnichannel has long been treated as a design and marketing challenge. Teams spend millions aligning mobile apps with websites, updating in-store kiosks, and coordinating campaign creative across sister brands. Yet, customer frustration remains at an all-time high.

The underlying issue is an architectural gap. Trust and security now outrank product quality as the primary reasons a customer creates an account. According to the [Auth0 Customer Identity Trends Report](#), 74% cite brand reputation and trustworthiness, while 72% cite strong security measures as non-negotiable requirements. Meanwhile, 62% of consumers cite long sign-up forms and disjointed login screens as their top digital frustration.

Underneath these visible symptoms sits a fragmented identity infrastructure: one login system for the website, an isolated database for the mobile app, and a completely disconnected loyalty platform for physical stores. The resulting mismatch between the customer data an enterprise holds and its ability to actually recognize that customer in real time is the **Recognition Gap**.

As autonomous AI agents emerge as a primary transaction channel across retail, travel, and financial services, this gap transforms from a user experience inconvenience into a total market lockout. Human customers might tolerate a redundant login prompt, but an AI agent acting on their behalf will simply fail and route the transaction elsewhere.

Closing the Recognition Gap for both human buyers and their AI agents is the true definition of omnichannel maturity.

The Recognition Gap — why omnichannel was always a backend problem

To understand why traditional cross-channel initiatives fail, we have to look past the user interface and examine how customer data is actually structured behind the scenes.

In a true omnichannel environment, a user who authenticates on a smart TV should be instantly recognized on their mobile companion app. A traveler who books a flight online should have their loyalty status immediately reflected at the physical check-in kiosk. A banking customer who starts a mortgage application on their phone should be able to finish it securely on a desktop browser without starting over.

Instead, most consumers face constant amnesia. They are forced to re-identify themselves at every new touchpoint, proving who they are over and over again to the same parent company.

This friction has a direct commercial cost across every major B2C sector:



Retail and E-Commerce

Nearly a quarter of shoppers regularly abandon purchases due to sign-up friction. Among Gen Z and self-identified “Tech Innovators,” this abandonment rate reaches 43%. At the checkout phase specifically, 26% of US shoppers walk away because the site forced mandatory account creation, equating to \$230B of recoverable revenue.



Financial Services

Banks remain the most trusted institutions for securing personal data (63% consumer trust). Yet, 78% of financial institutions with unified digital banking already in production still rely on self-built, legacy identity infrastructure that cannot share real-time context securely across web, mobile, and branch systems.



Travel, Hospitality, and QSR

...w that demand too much personal information up front. When a hotel guest or restaurant diner is forced to create separate accounts for web booking, mobile check-in, and reward tracking, loyalty engagement drops off significantly.



Media and Entertainment

Streaming subscribers frequently churn when cross-device authentication fails, or when sibling brands under the same media conglomerate force them to maintain multiple subscriptions and separate credentials.

The ambition vs. execution gap

Industry Vertical	Strategic Ambition	Architectural Reality
Retail & E-Commerce	Cross-channel strategy is the top growth priority	78% operate with siloed, channel-specific user databases
Financial Services	Deliver unified digital banking and wealth management	78% rely on pre-CIAM, legacy identity architecture
Travel & Hospitality	Seamless “couch-to-cabin” guest recognition	54% lose users due to excessive, disconnected profile forms
Media & Streaming	Unified multi-brand content ecosystems	Users maintain separate logins for sister networks and apps



20%

Estimated percentage of e-commerce tasks in 2025 already handled by agentic AI

1,200%

year-over-year increase in AI-referral traffic to US retail platforms

The emerging threat of agentic exclusion

While human shoppers create immediate friction leaks, the rise of agentic AI introduces an entirely different category of risk—one that is absolute and invisible: Agentic Exclusion.

We are already seeing the foundation of this shift. Consumers are rapidly delegating discovery, comparison shopping, and routine purchasing to autonomous AI assistants. Today, an estimated 20% of e-commerce tasks are already handled by agentic AI, driving a massive 1,200% year-over-year surge in AI-driven retail traffic. This behavior is quickly scaling into a structural rewriting of the global economy: Bain & Company projects agentic commerce will command up to \$500 billion in US retail by 2030, while McKinsey estimates the global agent economy will reach \$5 trillion.

But here is the brutal reality of a machine-to-machine economy: An AI agent does not care about your brand.



When an AI agent attempts to execute a transaction on behalf of a human customer, it cannot read a brand's marketing emails or appreciate its UI design. It requires API-driven authentication, delegated permission access, and structured data validation. If your identity architecture cannot securely verify the agent, confirm user consent, or exchange short-lived tokens, the transaction fails instantly.

Unlike a human user who might contact customer support or try resetting a password, an AI agent operates silently at machine speed. It routes the purchase to a competitor with accessible, API-first identity infrastructure, cutting your brand out of the transaction entirely without ever generating a bounce metric or a support ticket.

From Recognition Gap to Recognition Advantage

Closing the Recognition Gap requires moving away from the assumption that omnichannel is a design discipline.

Historically, organizations approached digital growth by building channel-specific identity silos. This usually resulted in one of four legacy patterns:

1.

Homegrown code

Engineering teams manually hand-rolled authentication logic inside individual application repositories, creating brittle code that breaks during updates.

2.

Legacy IAM systems

Enterprise platforms built for internal employee management (B2E) were adapted for external customer flows, resulting in rigid, slow login boxes that cannot scale to consumer traffic.

3.

Bundled cloud utilities

Basic login tools bundled with cloud infrastructure providers were deployed, but lacked native support for complex, multi-brand federation or fine-grained privacy consent.

4.

Scattered point solutions

Separate vendors were hired for web login, mobile push verification, fraud detection, and loyalty management, scattering customer data across un-synced systems.

The modern paradigm treats Customer Identity and Access Management (CIAM) as an authoritative, real-time infrastructure plane. It acts as a single, continuously updated record of who a customer is, available identically to every channel, brand, and partner in real time.

The four pillars of modern omnichannel identity

To build an identity layer capable of supporting both human users and autonomous agents across diverse consumer sectors, enterprise architectures rely on four foundational design patterns:

1.

Unified multi-brand identity (Single Sign-On)

1. Unified multi-brand identity (Single Sign-On)

Customers expect a single set of credentials to unlock an entire brand ecosystem. Whether a user is booking a flight and a rental car under the same travel group, or accessing three different streaming services owned by the same media conglomerate, identity must be federated. Single Sign-On (SSO) centralizes the identity layer so a user logged into one property is instantly recognized across all affiliated touchpoints.

2.

Progressive profiling and contextual consent

2. Progressive profiling and contextual consent

Demanding a complete demographic profile during initial account creation triggers immediate drop-off. Progressive profiling captures minimal information at sign-up and uses dynamic prompts to collect additional preferences, loyalty details, and privacy consents over time as trust builds. Crucially, this data is written to the centralized identity layer, ensuring that a dietary preference recorded in a mobile app is instantly respected by the in-store ordering kiosk.

3.

Fine-grained, dynamic authorization

3. Fine-grained, dynamic authorization

Static Role-Based Access Control (RBAC) cannot manage the complex context required for modern omnichannel workflows or AI delegation. Modern infrastructure uses Relationship-Based Access Control (ReBAC) and Fine-Grained Authorization (FGA) to evaluate permissions at runtime based on real-time context—verifying exactly what a human user, a partner application, or an AI agent is authorized to do within a specific transaction window.

4.

Elastic, resilient infrastructure

4. Elastic, resilient infrastructure

Consumer identity infrastructure must handle extreme, unpredictable traffic swings, from retail flash sales and streaming sports premieres to holiday travel surges. An enterprise identity layer must offer high availability (99.99% SLA) and automated bursting capabilities to process millions of peak authentication requests without degrading latency.

“Now, each customer has a single Identity. We give them tailored customer experiences, but that doesn’t mean they need three different user IDs and passwords.”

Ramiya Iyer

GVP of IT Digital, Data and Pharmacy
Albertsons

“Before long, nearly all retailers will have to grapple with the fact that a significant percentage of their customers will not be human users but rather AI agents.”

Lareina Yee

Senior Partner and Director of Technology Research
McKinsey Global Institute

The Auth0 playbook — how identity becomes the growth engine

Transitioning from fragmented identity silos to a unified customer recognition engine requires an extensible platform that orchestrates user sessions across every touchpoint.

The Auth0 platform acts as this central identity layer, managing human authentication, risk analysis, data enrichment, and agent delegation out of the box.

Core platform capabilities for human journeys

Universal and embedded login

Unify authentication across web, mobile, smart TVs, and single-page applications using customizable, branded login interfaces that support Passkeys, biometrics, and enterprise federation natively.

Serverless extensibility (Auth0 Actions)

Development teams can inject custom serverless JavaScript logic directly into the authentication pipeline. This allows brands to query loyalty tiers, fetch points balances from external databases, or sync zero-party preferences into Customer Data Platforms (CDPs) in real time the exact millisecond a user logs in.

Seasonal bursting and SLAs

Built to sustain enterprise peak traffic spikes, Auth0 delivers 99.99% uptime SLAs through high-volume seasonal events, ensuring that backend identity servers never become the bottleneck during critical revenue windows.

The secure architecture for autonomous AI agents

Because 66% of consumers state they would refuse to let AI make purchases on their behalf, and 58% express concern over how AI handles personal data, agentic workflows must be backed by strict, auditable identity controls.

Auth0 delivers a structured six-step execution architecture to govern autonomous AI transactions securely:

Execution Step	Technical Mechanism	Operational Purpose
1. User Authentication	Passkeys / WebAuthn	Establishes the primary human identity and initiates a trusted, secure session
2. Session Context	OpenID Connect (OIDC)	Attaches the verified human identity and explicit user intent directly to the AI execution loop, ensuring the agent operates on behalf of a known user
3. Token Vaulting	Short-Lived OAuth 2.0	Stores, exchanges, and rotates permission-scoped tokens. This allows the AI agent to call downstream APIs (inventory, billing, booking) without exposing raw customer credentials
4. Fine-Grained Auth	Runtime Policy Checks	Evaluates transaction limits dynamically at request time. For example, an agent can check a flight status but cannot cancel a non-refundable ticket
5. Async Authorization	Out-of-Band Prompts	Triggers human-in-the-loop approvals (e.g., a push notification to a mobile device) for high-value purchases or sensitive profile changes
6. Cryptographic Audit	Identity-Attributed Logs	Records auditable trails mapping every machine API call back to both the executing agent ID and the originating human user

Quantifiable business impact

Transitioning to a unified identity foundation delivers measurable operational and revenue gains across the enterprise:

50% to 75% reduction in time-to-market

Organizations moving from legacy or homegrown identity to unified CIAM drastically cut application rollout timelines. Leading financial services firms have reduced the deployment of new digital banking portals from 18 months down to just 9 months, with some credit unions going from 4 months to 4 weeks.

Up to 80% reduction in support call volume

Centralizing account management and enabling self-service credential recovery dramatically reduces high-cost support tickets driven by fragmented, forgotten passwords.

Elimination of redundant engineering

Replacing point solutions with a single identity plane reduces custom code maintenance, simplifies compliance reporting across borders, and allows development teams to focus purely on core product features.

In practice: Customer results

The strategic value of unifying customer identity is proven across leading global consumer enterprises:



Dine Brands: Unifying multi-brand loyalty across 3,500 locations



Listen to [Auth0 Streamcast:](#)
[From Security Bottleneck to Revenue Growth Engine](#)

The Challenge

Dine Brands, parent company of IHOP and Applebee's, operated fragmented digital platforms across its massive footprint. Disjointed guest accounts created friction for cross-brand loyalty sign-ups, while custom security reviews for new digital features delayed rollouts by months.

The Solution

Standardized on Auth0 as their enterprise identity plane, unifying guest logins, loyalty integrations, and security controls across both distinct restaurant concepts.

The Outcome

The platform now powers 14 million IHOP loyalty members and 17 million Applebee's loyalty members under one cohesive architecture. Security review cycles dropped from months to days, and the unified identity engine now serves as the secure foundation for an in-restaurant AI personalization pilot scaling across thousands of locations.

cinépolis



Cinépolis: Transforming media and entertainment onboarding

Read the [Auth0 Cinépolis Case Study](#)

The Challenge

Cinépolis, the world's fourth-largest cinema chain, relied on manual, disconnected physical box-office registration for its loyalty program. This created long lines, siloed customer databases, duplicate accounts, and high fraud rates.

The Solution

Retired legacy identity infrastructure and deployed Auth0 to power a seamless, self-service mobile and web onboarding experience, backed by automated phone validation and fraud defense.

The Outcome

The transition to a unified digital identity layer resulted in 1.3 million new loyalty members in just three months—a 300% increase in net-new loyal customers. Furthermore, centralized visibility helped reduce fraudulent transactions by 16%.



Jersey Mike's Subs: Rapid rollout for 15 million+ consumers

Read the [Auth0 Jersey Mike's Case Study](#)

The Challenge

To meet surging digital demand, Jersey Mike's needed to overhaul its mobile application and digital ordering pipeline across 1,900+ locations without forcing millions of existing loyalty members to reset their passwords or re-enter billing details.

The Solution

Implemented Auth0 to execute a secure bulk user migration, establishing a single identity layer for digital transactions across web, mobile, and in-store channels.

The Outcome

The brand went live in under 90 days, securing over 15 million customer accounts seamlessly. As CIO Scott Scherer noted: "With Identity security taken care of, our engineers can spend more time creating new user experiences."

Key takeaways

Every dollar spent designing a consistent front-end experience on top of a fragmented identity backend is capital spent painting over a cracked foundation. As agentic AI transforms how consumers interact with digital platforms across retail, finance, media, and travel, that fragmented foundation will be stress-tested across every channel simultaneously.

Bringing it back to your team

You don't need to overhaul your entire enterprise architecture overnight to start making progress. But before you commit more capital to front-end channel redesigns, it pays to get a clear picture of where your identity layer currently stands.

Here is a quick diagnostic framework you can take to your next product, engineering, or digital leadership meeting:

1.

Map your true recognition

Audit your primary touchpoints alongside your engineering team. Ask a simple question: *When a customer moves from our web store to our mobile app, physical location, or partner brand, do we recognize them instantly as one continuous person, or are we relying on visual tricks over disconnected databases?*

2.

Quantify your hidden friction

Work with your analytics lead to measure the exact drop-off at your registration screens, password reset prompts, and loyalty sign-up boxes. Calculate how much revenue and repeat business you are losing simply because identifying oneself feels like an administrative chore.

3.

Test your system for AI readiness

Ask your technical architects whether your current identity layer can issue short-lived, permission-scoped tokens to external AI agents acting on a customer's behalf. If an autonomous assistant tried to buy something on your platform tomorrow, would your backend authenticate it—or block it?

Take the next step

Closing the Recognition Gap ensures your best customers—and the AI tools they rely on—are recognized, protected, and empowered everywhere they engage with your brand.

Run your diagnostic

Download [The Digital Drop-Off Audit Checklist](#) to evaluate your current sign-up, login, and multi-channel flows against modern conversion standards.

Explore cross-industry solutions

Discover how specialized identity infrastructure powers seamless experiences with [Auth0 for Retail](#) and prepares your architecture for autonomous transactions with [Auth0 for AI Agents](#).

Talk to an Auth0 Architect

[Schedule a technical scoping session](#) with our engineering team. We will help you evaluate your current identity stack and design a unified path forward for the customers you have today—and the AI agents that will transact on their behalf tomorrow.

