SECUREAUTH
Welcome to Better Identity.

eBook

Transaction Authorization for Retailers

Delight Customers, Grow Revenue, Reduce Costs with Best-in-Class CIAM

Get Started

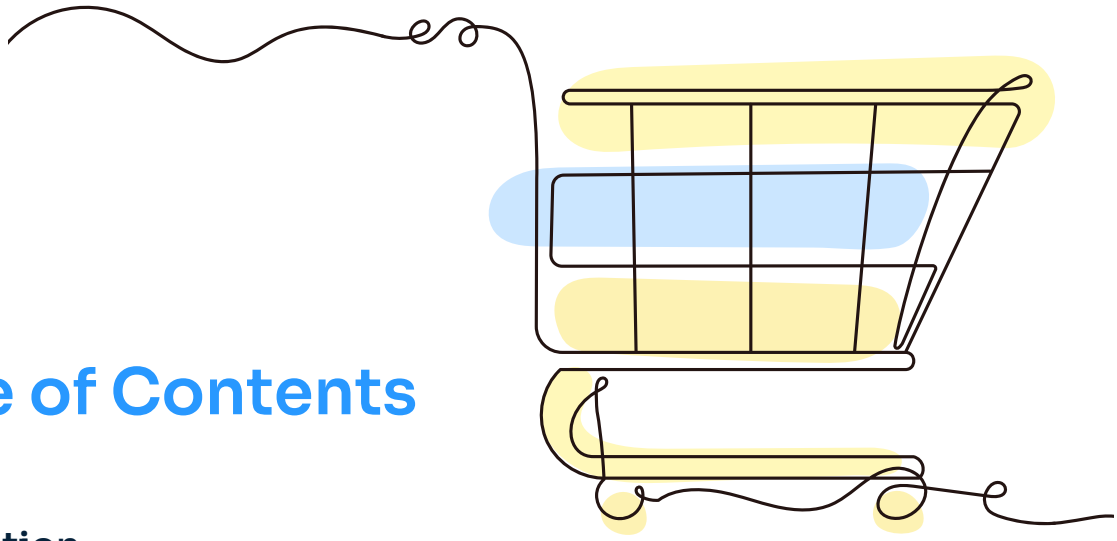


Table of Contents

Introduction

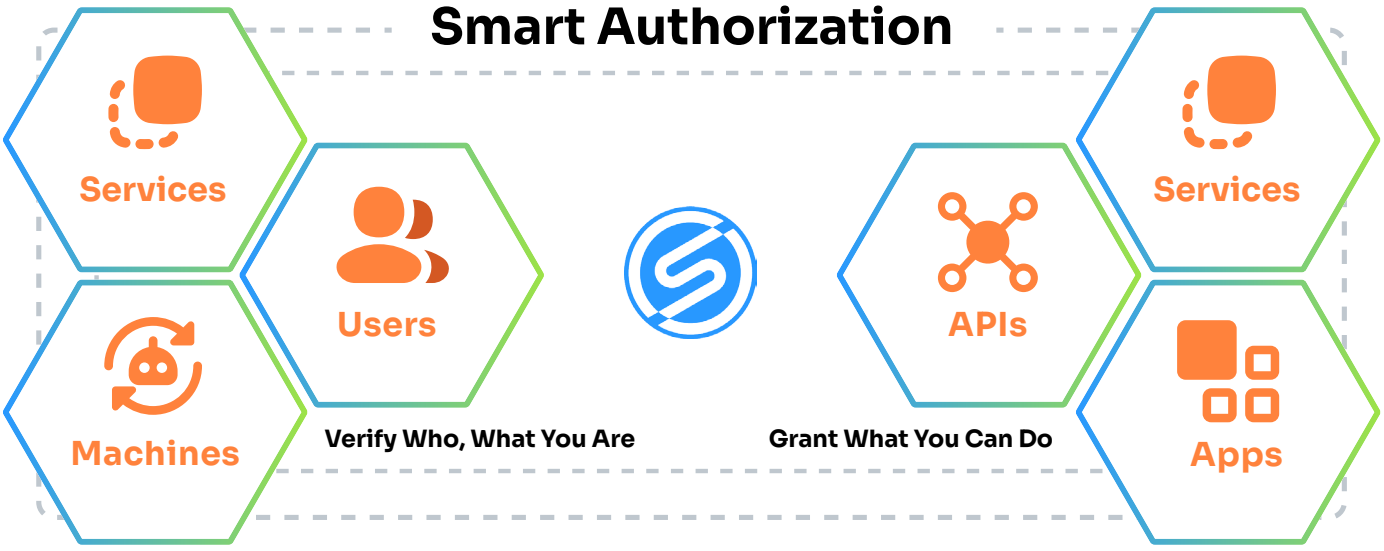
Leading and emerging retailers have three primary objectives when it comes to driving online business growth while ensuring the highest levels of security for their customers.

Customer Growth
Adding new customers at scale, retaining existing customers, and increasing the spend per customer

Reducing security and infrastructure costs

Providing friction-free experiences

SecureAuth's identity and authorization solution provides retailers of all sizes with a standards-based and non-disruptive approach to address these needs while also accelerating innovation to delight their customers.



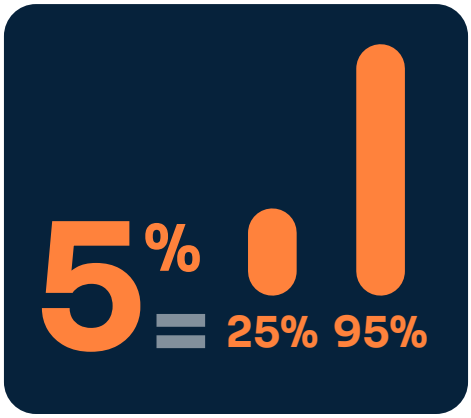
SecureAuth delivers fine-grained, intelligent authorization with industry leading performance in a cloud-first platform that is easily automated. The SecureAuth solution is available as a SaaS or can be deployed anywhere you need it: in the cloud, hybrid environments, or on-premise.

Current State of Retail CIAM

Many retailers have a homegrown CIAM environment built from custom components and common industry-standard gateways. However, this type of environment does not provide fine-grained access control or transactional MFA based on real-time fraud and transactional context, to mitigate risk in real-time. These controls are necessary to substantially reduce fraud while maintaining a positive customer experience and reduced user friction.

Much of the current infrastructure that retailers are using needs to be modernized to enable faster innovation and bring new services to customers that are highly secure, reduce fraud, add new revenue streams, or remove friction from new services and business opportunities. This must be accomplished while avoiding heavy friction on developers and customers from a “big bang” update requiring millions of customers to update their mobile apps.

Research shows that increasing customer retention rates by 5% increases profits by 25% to 95%



$213 B

Opportunity for businesses willing to reduce customer friction

The Baynard institute estimates that reducing customer friction is a $213 billion opportunity for businesses in the U.S. alone, and Brain research shows that increasing customer retention rates by 5% increases profits by 25% to 95%. These potential business outcomes are critical factors in considering your identity management experience.

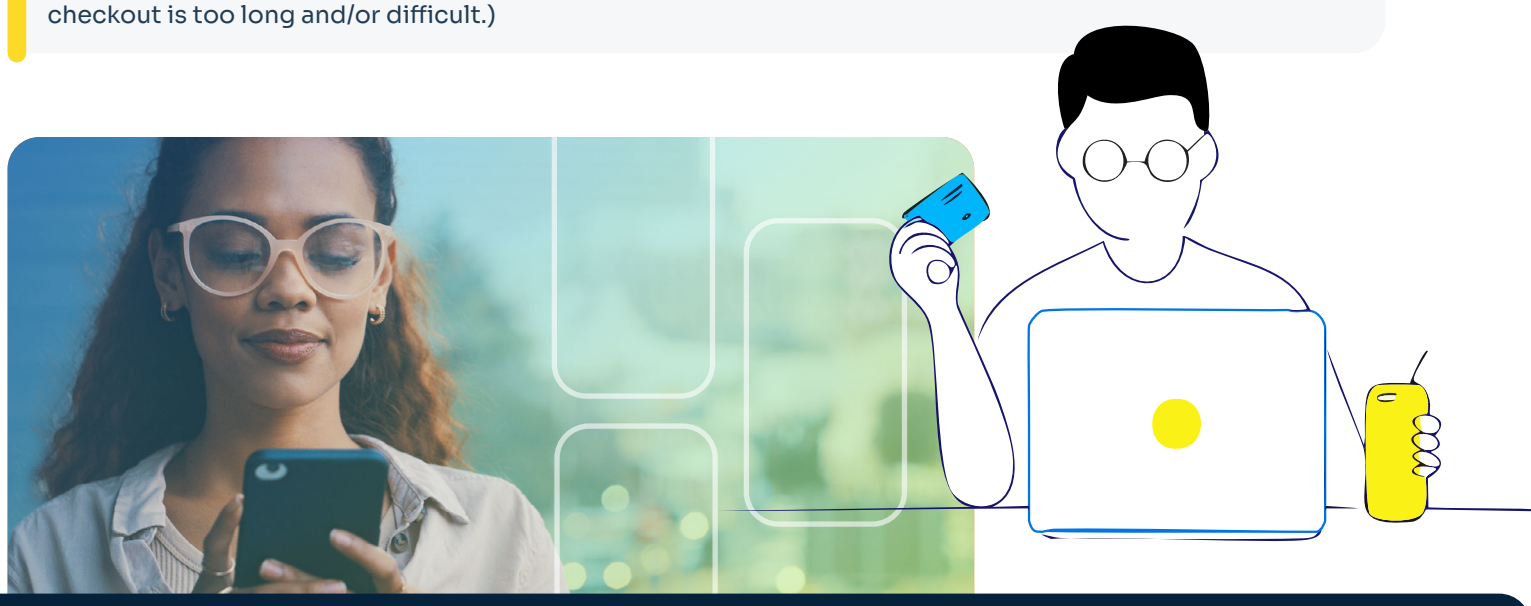
Retailers should consider solution options that are standards-based to ensure compatibility, interoperability, and future-proofing. This facilitates easier integration with existing systems, reduce vendor lock-in, and adhere to industry best practices, enhancing security and scalability while supporting innovation and flexibility. Additionally, the scalability, growth, and performance of these solutions should be considered to address both current and future needs.

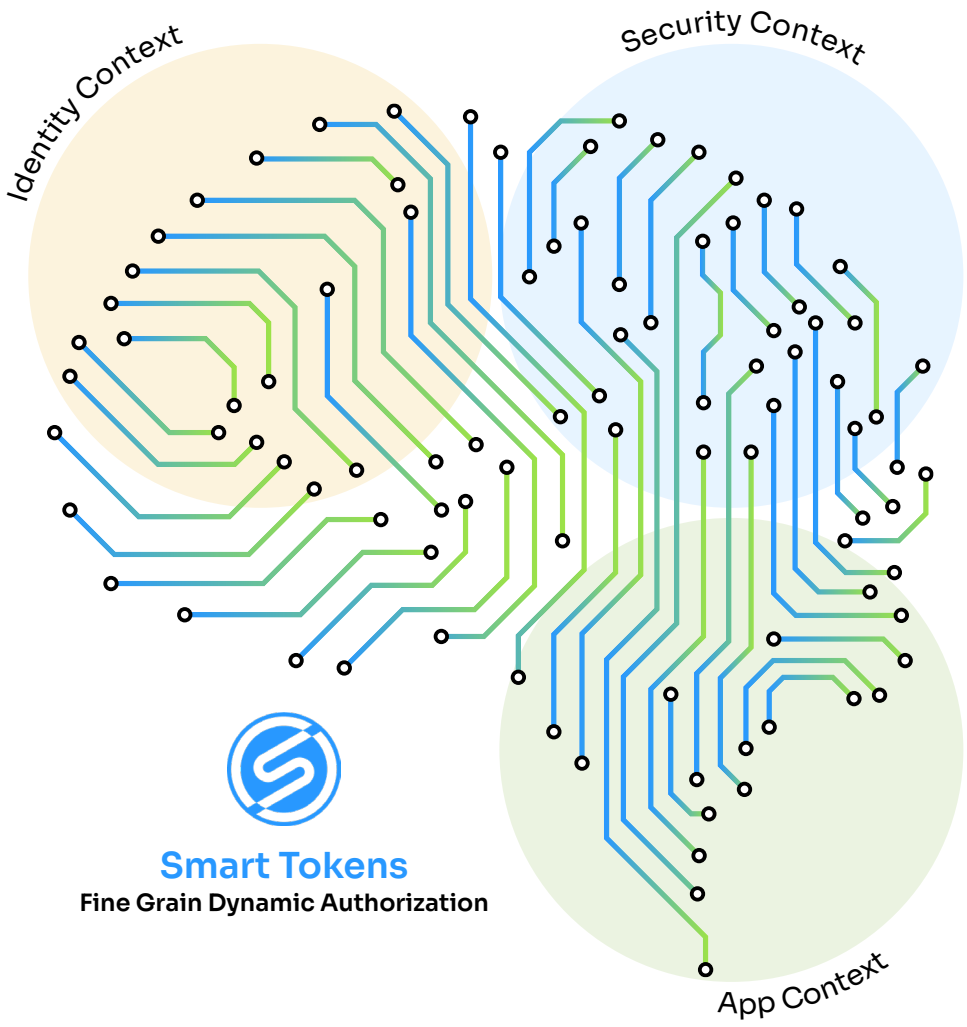
How SecureAuth Helps Retailers Drive Revenue Outcomes

SecureAuth uses contextual, fine grained access controls to create dynamic, friction-free customer experiences. With SecureAuth the business no longer is forced to choose when it comes to security vs customer convenience. SecureAuth adds additional context from fraud engines, existing entitlement stores and other cybersecurity solutions to intelligently orchestrate the customer journey without changes to the application code. This allows customers to be unencumbered by security constraints such as MFA or data collection until the exact point in the transaction security requires it. This approach lets customers do more, spend more, register more efficiently and honor their privacy, without adding extra friction unless necessary.

The context that SecureAuth aggregates allows retailers to incorporate more knowledge about their customer; things like trusted device, the last time they strongly authenticated, changes in network access, changes in client app, and thousands of other factors are used to dynamically update the customer journey and means customers will have less friction and be able to perform transactions more freely with higher assurances of security and less fraud. Fine grain access control at a transactional level creates the ability to more stringently authorize high dollar value actions during the checkout process such as reloading a gift card in conjunction with other transactional context resulting in lower fraud rates and increased customer retention.

> (87% of consumers consider the checkout process one of the biggest friction points during a purchase. 70% of customers leave their online shopping basket due to friction (e.g., they need to create an account or experience restricted pay methods). 28% out of that 70% abandon their purchase because the checkout is too long and/or difficult.)





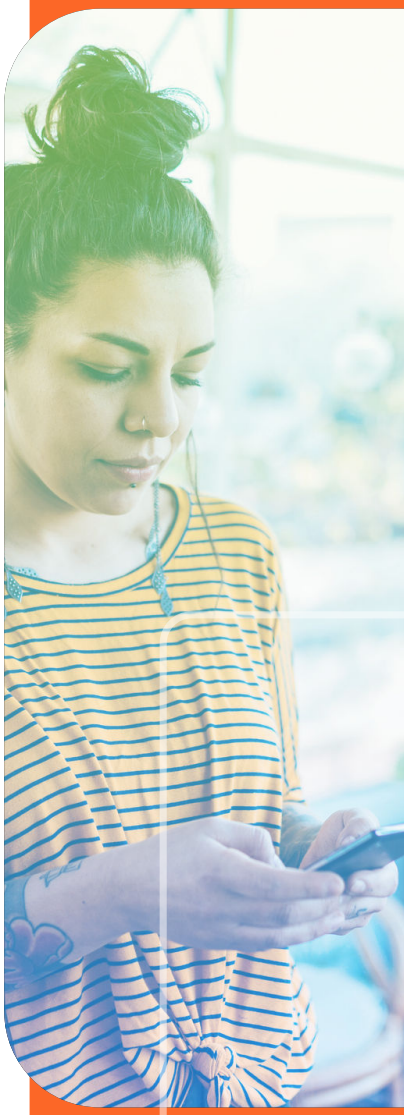
In addition, SecureAuth facilitates the capture and management of fine-grained consent for transactions, which is critical for customer acquisition and retention. Studies show that when customers feel their privacy is respected, they are more likely to engage with that business activating on new offerings (Microsoft Commissioned Study - The Consumer Data Value Exchange). Trust builds brand loyalty and trusting Customers share more data, consume more services creating a positive feedback loop with retailers and their partner ecosystem that drives customer LTV. (Good Friction Applied, Forrester)

Reduce Security and Infrastructure Costs

Authorization is often a manual process at retailers, that is hard coded into the applications. In order to drive efficiency and streamline time to market, retailers must adopt an externalized, declarative authorization model using centralized management with distributed enforcement. This allows application team A to easily and securely consume Application team B's policies, user consents and associated APIs AND allow security to audit usage and compliance of that data.

Fraud Protection

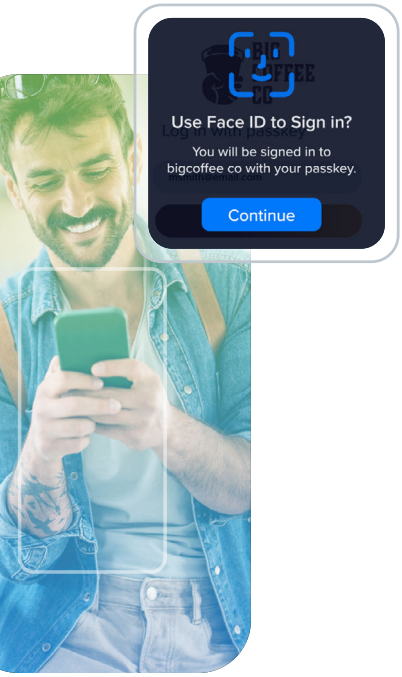
SecureAuth's policy-based fine-grained access controls allows retailers to invoke existing MFA for high value transactions. For example, different MFA mechanisms can be applied based on contextual factors or specific dollar amounts reload on a gift card etc. SecureAuth also includes a built-in behavioral risk engine that continuously monitors user activities, providing real-time risk scores to drive authorization access decisions based on policies and the actual transaction authorization request itself. SecureAuth can incorporate other fraud data or risks scores from other sources, adding another layer of dynamic fraud protection.



Transactional Authorization

SecureAuth decouples authentication from authorization, enabling applications to request transaction-level authorization using the advanced profiles within the OAuth 2 and OIDC open standard specifications. These transactional authorizations adhere to security policies that consider the context of not only the user, but also specific transaction details and the conditions under which the authorization is requested. Authorization requests originating from applications can be represented in an open standard format, enabling adherence to open specifications. The transaction authorization policies are centrally controlled and enforced within the SecureAuth platform, allowing for fine-grained access evaluation and the issuance of authorization grants for specific transactions.

The ability for retailers to make a real-time decision about which transactions require additional authorization (and therefore additional friction for the end-user) and which ones don't, is the key to balancing end-user friction with safety for both the business and the end-user. SecureAuth gives the business the flexibility to tailor security policies and mitigation tactics to the specific risks and fraud patterns they are facing as well as the centralization and manageability to control and govern these policies at scale.



Developer-Friendly Integration

SecureAuth enables developers and security teams to specify permissions and policies in an easy to manage, declarative manner. All policies can be created and manipulated using our no-code graphical editor.

We offer an API-first approach for seamless lightweight integration into existing infrastructure and DevOps pipelines, empowering your business to shift-left and enable developers to control how their applications leverage SecureAuth's authorization capabilities. Since all SecureAuth integrations and configurations can be represented as code, adopting a GitOps deployment approach to manage policies via a CI/CD pipeline is straightforward.

SecureAuth deploys directly in existing environments, integrating seamlessly with existing environments and Authentication providers. Our standards-based approach allows us to work with multiple IDPs, multiple API Gateways and other solutions in your environment to add more contextual intelligence from identity data, security context, fraud engines and more.

Build vs. Buy: Why not save money and build it yourself?

Applications are becoming more and more complex with user mobility, multiple SaaS and multi-cloud environments. In addition, business needs to respond more quickly to the fast-changing environment of today's mobile and multi-device users.

The core considerations to weigh in a build versus buy scenario:

- While adding features that delight your partners and customers, how will you protect against the onslaught of API threats and fraud?
- How do you drive revenue, reduce costs, retain customers and increase security?
- Do you divert your dev talent from applications to Authorization?
- Do you have the specialized resources needed to develop a secure and scalable authorization function for your applications?
- Do they have visibility into the latest innovations and evolving specifications within the identity and authorization community, so that you're not relying on older standards?

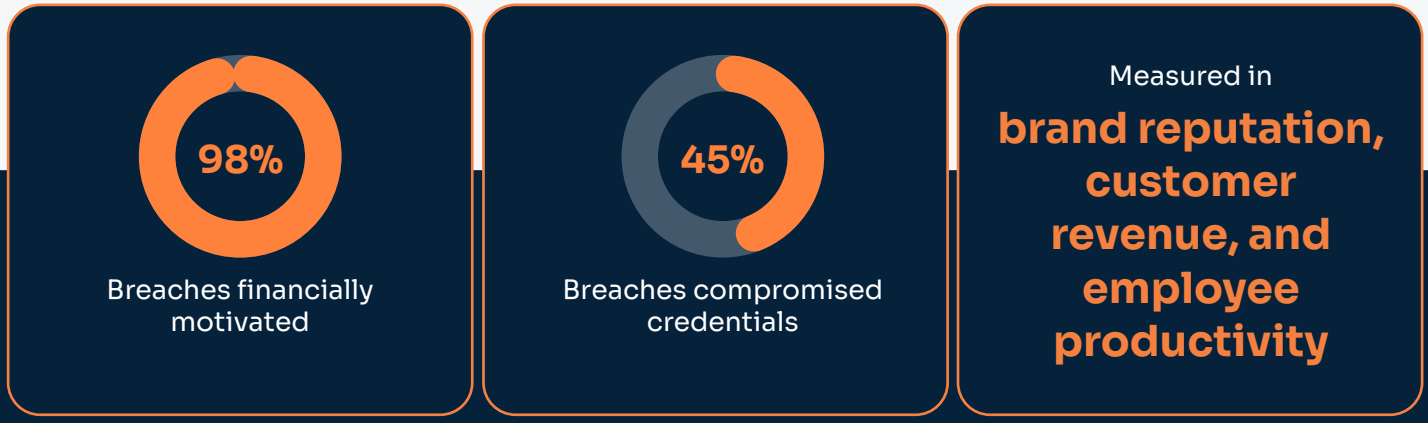
The Hidden Costs of Building In-House

Developers often feel that they have the expertise and bandwidth to add the development and management of Authorization Services to their personal workload. They are talented and feel they can deliver an additional capability or solution on time and within budget.

The hard reality is that developers often overestimate their capabilities (in terms of the speed they can code at) or underestimate the project (in terms of complexity). They usually have just a few hours to estimate all the hours they and their team will need to work over 4 to 6 months of development. This underestimating of hours and even tools needed, are a hidden cost that can grow quite rapidly and delay rollouts substantially. This could be described as The Planning Fallacy. The Planning Fallacy is a specific form of Optimism Bias, where we have a tendency of underestimating adverse variables that could impact our performance and, therefore, we predict far favorable results than what is most likely.

This under estimation of hours needed is not due to a lack of talent. Some developers get behind in in project A so they get optimistic on project B to make up for lost time.

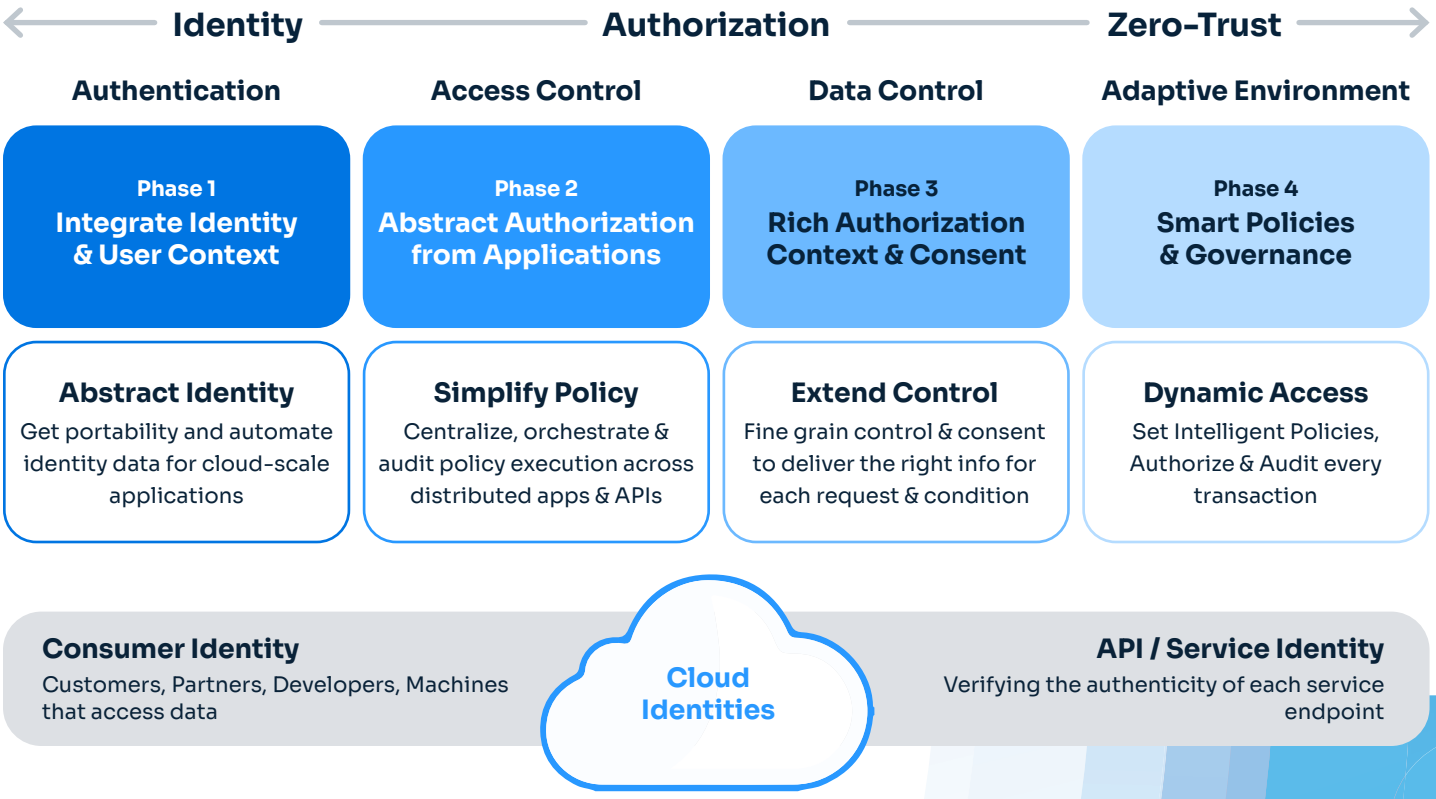
Companies must constantly monitor, maintain, and patch their code and libraries to ensure user data is secure. Often development teams don't update security aspects in a timely manner. Network and application security tend to live in different parts of the organization. Apps accumulate technical debt as developers race to meet other deadlines. All this can result in potential security vulnerabilities in your app.



Bottom Line: For most organizations the answer becomes clear. Retailers should focus on building business value in their areas of expertise and buy proven solutions and infrastructure to address their mission-critical security needs.

A Unified Solution

SecureAuth provides a unified solution to control data access across your entire modern application journey, from integrating identity data to ensuring that every API call is authenticated, authorized and governed. We take the headache out of authorization, enabling cloud-native applications and a zero-trust access model to better protect API data.



We take the headache out of authorization, enabling cloud-native applications and a zero-trust access model to better protect API data.

The SecureAuth Difference for Retailers

01

Open Standards Solution

SecureAuth is built leveraging "Open Standards" technology, not a proprietary tool set, so it is easily adoptable by the Business, DevOps and Security. OAuth, OIDC, SPIFFE, OPA

02

Integration with Existing IDP and Data Sources

Use context from any IDP, token, database, security solution, etc. for dynamic Authorization SAML and OIDC tokens plus REST, SCIM, LDAP, SQL, NoSQL or GraphQL data stores.

03

Multi-Tenant & Delegated Admin

Control Client-Partner access without needing to manage partner's IDP or individual partner's users.

04

Fast Deployment

Deployed as a "Public or Private SaaS Solution" and takes full advantage of Kubernetes in Service Mesh.

05

Scale

Evaluate and mint 100,000+ tokens per second

06

API & Service Discovery

Discover and catalog API's automatically and easily assign policies to new API's.

07

Dynamic Data sharing

Create dynamic authorization-based business agreements with partners and govern/authorize attribute flows between partner and customer organizations

08

Machine to Machine Transactions

Policies that govern not just what a Machine can see but also what it can share to other APIs

09

Governance of Policies, Tokens & Data

Full audit and reporting of all policies, tokens and data authorized to an endpoint. Adhere to privacy and data sharing requirements with simple updates.

10

Consent Management and Authorization

Insert consent and consent-based authorization directly into existing services to dynamically change the user journey. Provide fine-grained management of user consent and data.

Key Takeaways

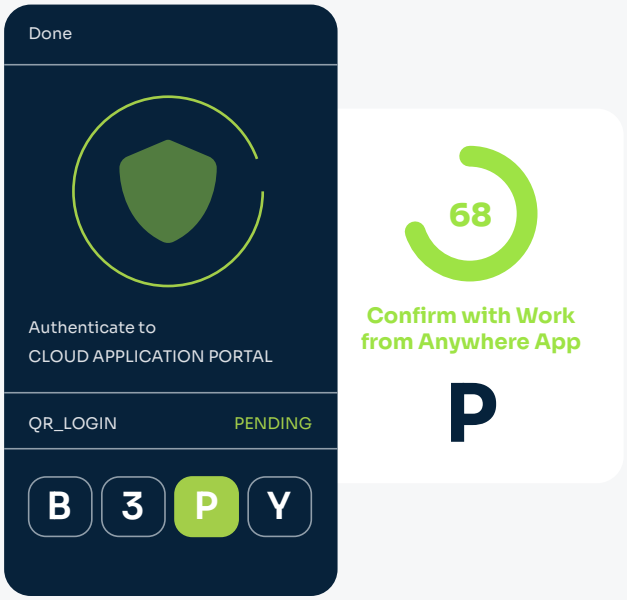
Partnering with SecureAuth, retailers can utilize our Authorization as a Service across many of your teams to increase revenue, reduce fraud, reduce internal costs and increase the velocity of new applications and innovation to delight your customers. This can be accomplished without a deployment “big bang” and disrupting your customers and your revenue stream.

Increase Revenue and Reduce Fraud for the Business

- Faster time to market with new offerings that drive revenue.
- Enhanced services and user experience to improve the customer journey, retain customers and increase revenue streams.
- Eliminate security barriers to new business so customers can quickly and securely on-board, removing friction by using context.
- Reduce fraud by adding friction where needed, like an MFA for high-dollar gift card re-loads.

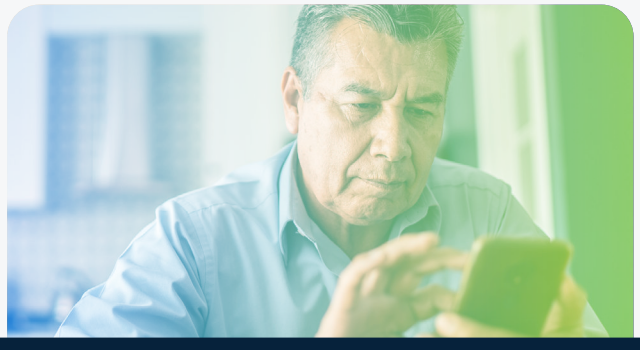
Reduce Cost in Development

- Reduce authorization coding effort, complexity, human error.
- Offload development security and compliance overhead.
- Standardize declarative authorization policy as code.



Improve Security and Process in DevSecOps

- Expedite app security verification time and effort.
- Standardize policy oversight, gain continuous enforcement.
- Mitigate attack, data leakage and compliance risk.



Take the Next Step

SecureAuth has deep expertise and a long history of working with retail customers. Retail customers using our CIAM solutions are able to create new policies that drive dynamic customer journeys with fine-grained consent, intelligent authorization.

See for yourself. Book a demo or request a free trial of our CIAM solutions today.

Book a Demo **Request Free Trial**

About SecureAuth

Welcome to Better Identity
We believe more security shouldn't equal more obstacles.

And, with Identity Management solutions from SecureAuth, leading companies worldwide find it easier than ever to create experiences that are as welcoming as they are secure.

Our AI-driven risk engines help you bring dynamic —and often invisible — authentication for your audiences. Making you more effective than ever at eliminating bad actors or incorrect authorizations. While providing your employees and customers the simple and seamless access they deserve.

Make all your authentication user experiences a secure and accessible "front door" to your company.

Visit SecureAuth.com to learn how.