SECUREAUTH
Welcome to Better Identity.

eBook

Protecting Users from Account Takeover, Phishing, and Credential Theft with Proper CIAM Architecture

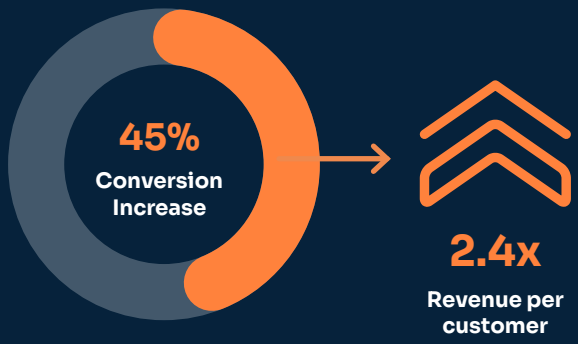
Get Started

Table of Contents

Introduction

Customer Identity and Access Management (CIAM) is a critical component for businesses that interact with customers online. A robust CIAM architecture ensures seamless and secure access for legitimate users, protects against various security threats such as account takeover, phishing, and credential theft. The upside of creating trusted seamless experiences is also clear. Studies have shown that improving the online registration experience alone has been shown to increase consumer conversion rates by 45%[1] and good versus poor online experiences net 2.4x revenue per customer.[2] This whitepaper explores how a proper CIAM architecture can safeguard a business's users from these threats while maintaining delightful user experiences, with insights from SecureAuth.

Studies have shown that improving the online registration experience alone has been shown to increase consumer conversion rates by 45%[1] and good versus poor online experiences net 2.4x revenue per customer[2]



Understanding CIAM

CIAM systems are designed to manage and secure customer identities, offering features like authentication, authorization, user profile management, and data privacy. Unlike traditional IAM systems, CIAM focuses on external users, providing a seamless and secure experience across multiple channels and devices.

[1] Adaptive Path Study large retail bank.
[2] Harvard Business Review & Medallia analysis.

The Threat Landscape

Phishing

Phishing involves tricking users into divulging sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity. This is typically carried out through emails, fake websites, or social engineering.

Credential Theft

Credential theft is the unauthorized acquisition of user credentials, often through methods such as data breaches, keylogging, or man-in-the-middle attacks.

Account Takeover

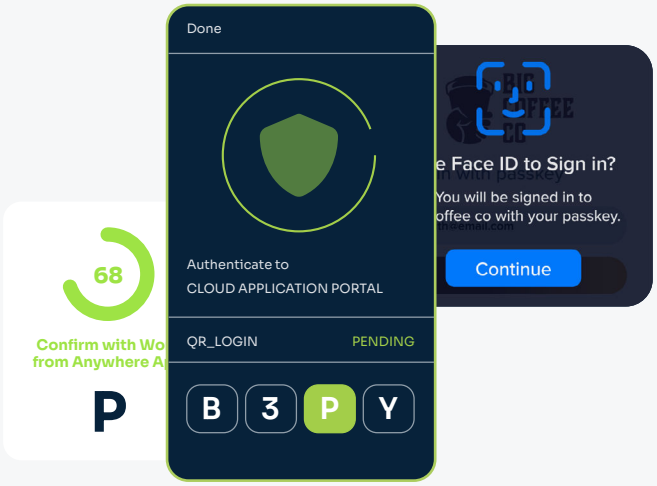
Account takeover occurs when a malicious actor gains unauthorized access to a user's account. This can result from weak passwords, phishing attacks, or the reuse of credentials across multiple sites.

CIAM Architecture for Protection

A well-architected CIAM system integrates various security measures to protect users from these current threats. The following sections detail the essential components and practices that contribute to a secure CIAM framework.

Phishing Resistant MFA

MFA (Multi-Factor Authentication) is a critical layer of security that requires users to provide two or more authentication factors to gain access. By combining something the user knows (password), something the user has (security token), and something the user is (biometric verification), MFA significantly reduces the risk of account takeover and credential theft.

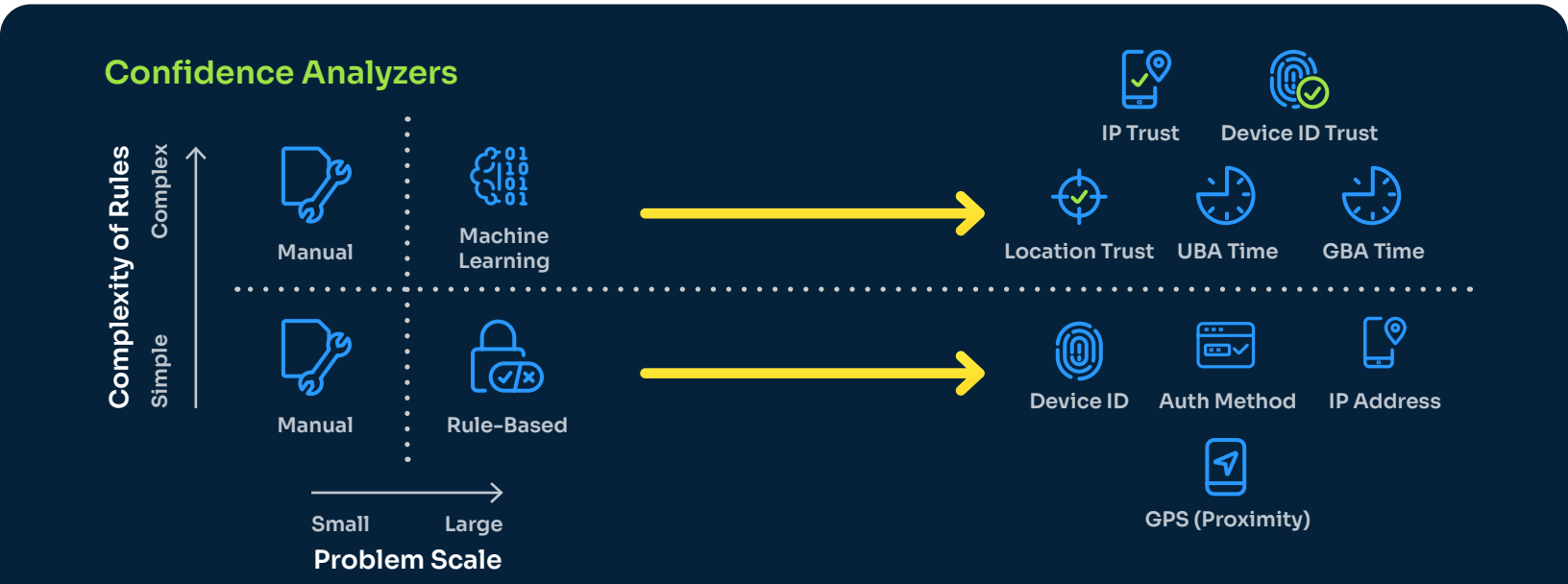


SecureAuth provides direct integration with over 30 of the latest and most popular MFA mechanisms, including those supporting the FIDO2 WebAuthn standards which can be used to bind URLs and Devices to specific authentication requests to further mitigate the risk posed by even the most sophisticated phishing and man-in-the-middle attacks.

Adaptive Authentication

Adaptive authentication dynamically adjusts the level of authentication required based on the risk associated with an interaction. Factors such as the user's location, device fingerprint, and user behavior patterns are analyzed to detect anomalies and impose additional verification requirements (such as MFA) when necessary.

SecureAuth's approach to adaptive authentication is to generate a Level-of-Assurance (LOA) score representing each transaction, which is used to determine the type and number of authentication mechanisms that need to be employed to sufficiently safeguard that transaction. The LOA score is generated by a constantly evolving machine learning model that considers over 20 characteristics of the user's device and/or browser to formulate a complete fingerprint, as well as User Behavior Analytics (UBA) which track and analyze user activities to identify deviations from normal behavior for the individual user, as well as across the entire user population. When the calculated LOA does not meet the requirements of the policy configured for a particular type of request, the interaction is considered a potential threat which triggers the dynamic increase of authentication friction in real-time. Similarly, a high LOA score can trigger a reduction in friction to provide a smoother and easier experience for non-threatening user interactions.

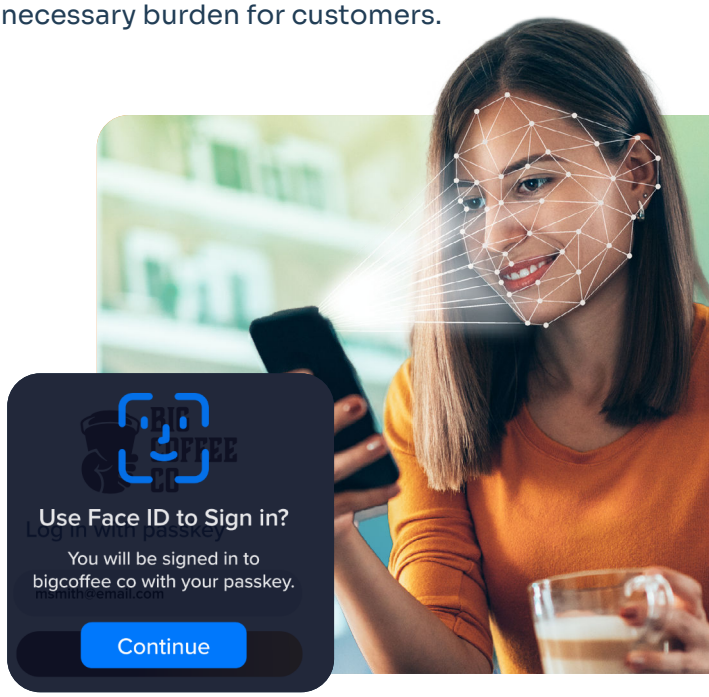


Passwordless Authentication

Passwordless authentication methods, such as biometric authentication or magic links, eliminate the need for traditional passwords, reducing the risk of phishing and credential reuse. SecureAuth emphasizes the importance of implementing passwordless authentication to enhance security while improving user experience. True passwordless CIAM implementations that do not require end-users to install software can be quickly and easily deployed using SecureAuth, without unnecessary burden for customers.

Threat Intelligence and Monitoring

Continuous monitoring and threat intelligence are vital for detecting and responding to suspicious activities in real-time. Mature CIAM systems incorporate advanced analytics and machine learning to identify patterns indicative of potential attacks. In addition to using AI/ML modeling to dynamically adapt to identity-related threats in real-time, SecureAuth's CIAM solution also leverages best-in-class threat detection and monitoring technologies to provide proactive threat and risk mitigation in an infrastructure-wide manner.

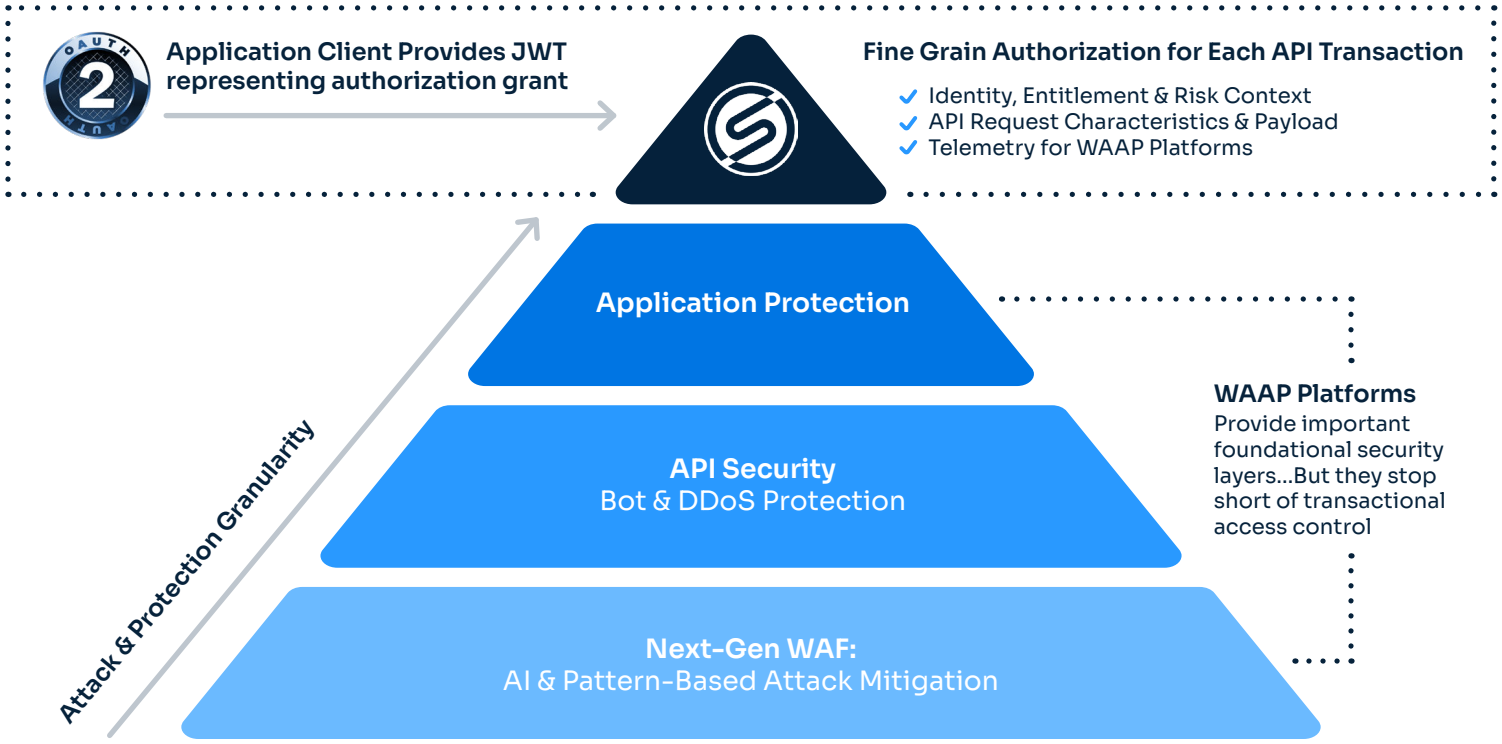


APIs are also the primary attack surface for most account takeover attacks

Secure API Access Control

APIs are the backbone of modern applications, facilitating communication between different systems. APIs are also the primary attack surface for most modern data exfiltration and account takeover attacks. One example that made headlines in 2018 was when a U.S. Postal Service API flaw exposed the data of 60 million customers. Normally, the attack's intent is not just getting logged in as the target user but performing transactions against these APIs while impersonating that user. Ensuring a strong API security posture that includes granular access control at the service edge is crucial to prevent unauthorized access and data breaches. Many businesses rely solely on WAAP (Web Application & API Protection) systems to protect their APIs; these solutions provide essential security tools such as WAF (Web Application

Firewall) for protection against AI & pattern-based attacks, API security controls to provide protection from Bot and DDoS attacks, and in some cases even application protection schemes that can fend off account takeover attempts. What WAAP solutions lack, however, is visibility into the identity-related elements of the API request such as authorization tokens that are used to control granular access to APIs. SecureAuth offers comprehensive identity-aware API access control that works with WAAP systems by consuming telemetry from the WAAP platform as well as providing audit-level information to the WAAP platform to enhance the level of control at both systems and ensure fine grained authorization for each API transaction. The solution is enabled by employing SecureAuth CIAM (which boasts the most complete OAuth 2 implementation on the market today) as well as distributed Microperimeter® policy decision points that can be deployed at/near the API service edge, to protect sensitive user data and maintain secure interactions between applications with the finest levels of granularity with extremely low latency.



Data Encryption and Privacy

Protecting user data through encryption both at-rest and in-transit is essential for safeguarding against credential theft. Additionally, ensuring compliance with data privacy regulations, such as GDPR and CCPA, builds user trust and reduces the risk of data protection lapses. SecureAuth's CIAM platform provides robust encryption and privacy features via the implementation of the latest security

and consent profiles such as Financial-grade API (FAPI) 2.0, as well as the specifications associated with many existing Open Finance and Open Data ecosystems such as FDX and CDR, to secure user information and ensure that the end user has complete control over the way their private data is disclosed and distributed.

User Education

Educating users about the dangers of phishing and credential theft is crucial. A CIAM system can integrate training modules and regular updates to inform users about the latest threats and best practices for maintaining account security. Encouraging users to recognize phishing attempts and report suspicious activity can significantly reduce the effectiveness of such attacks. SecureAuth stands ready to provide materials and/or hands-on assistance in generating the required educational strategies and materials to ensure your users are armed with the information they need to protect themselves.

Educating users about the dangers of phishing and credential theft is crucial.

SecureAuth sample tip sheet to help educate your users on guarding against account takeovers.

01 Stay alert—phishing attacks are everywhere, every day

Don't click on suspicious links or open attachments from unknown sources. Verify the authenticity of emails requesting sensitive information by contacting the organization directly.

02 Guard against social engineering—it's more common than you think

Stay vigilant against attempts to manipulate you into revealing confidential information. Verify identities before sharing sensitive information, even with people who appear to be trusted contacts.

03 Enable multi-factorauthentication (MFA) whenever you can

Use MFA wherever possible, preferably with an authenticator app rather than simply using SMS-based verification.

04 If passwords are required, make sure they are strong and unique

Avoid using easily guessable information like birthdates or common words. Each account should have a unique password to prevent credential stuffing attacks.

05 Keep them fresh—update and change your passwords often

Change passwords periodically, especially after any potential breach and avoid reusing old passwords.

06 Let a password manager do the heavy lifting

Store and generate strong passwords using a reputable password manager to ensure secure and unique credentials for each account.

07 Monitor your accounts for suspicious activity

Regularly review account activity for any suspicious or unauthorized transactions. Set up alerts for unusual login attempts or changes to account settings.

08 Stay ahead of the game—keep your software up to date

Ensure that all devices and applications are up to date with the latest security patches and software updates.

09 Be wary of public Wi-Fi

Avoid accessing sensitive accounts over public Wi-Fi networks. Use a VPN for an additional layer of security if needed.

10 Play it smart—choose your account recovery options wisely

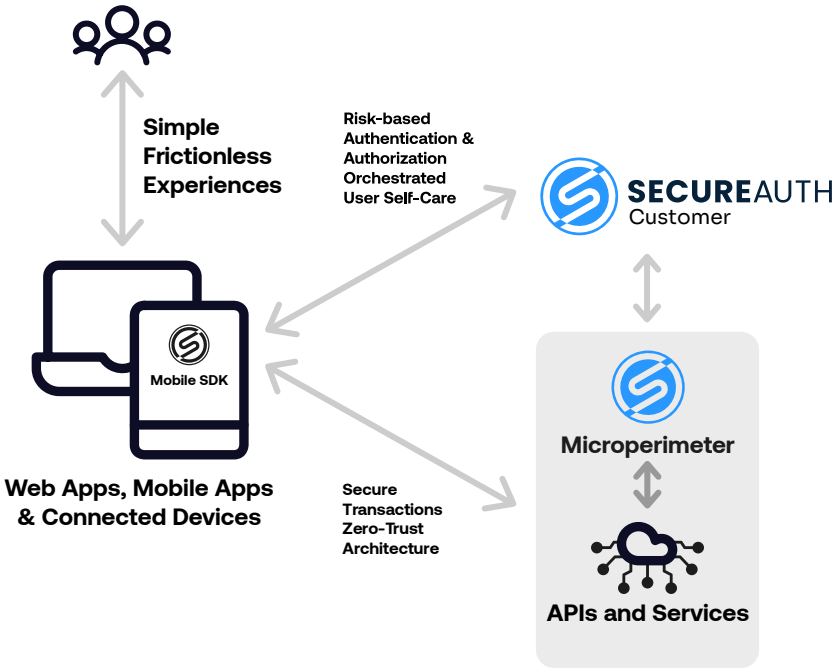
Set up secure account recovery options, such as secondary emails or security questions, and keep them updated. Avoid using easily discoverable information in recovery questions.

Mitigating Account Takeover Risk with SecureAuth's CIAM Solution

B2C CIAM: Built to Dynamically Reduce Friction

- Instantly Create Simple, Passwordless Experiences that Delight Users
- Dynamically control UX friction using AI/ML driven risk assessments
- Achieve Zero Trust by authorizing every sensitive transaction

- **The Lowest TCO**
- **The Shortest TTV**
- **The Best Experiences**
- **The Highest Security**



SecureAuth offers a comprehensive CIAM solution designed to protect users from account takeover, phishing, and credential theft. Key features of SecureAuth's CIAM architecture include:

- **Strong Authentication Methods:** Support for MFA, adaptive authentication, and passwordless authentication
- **Secure API Access Control:** Implementation of industry-standard protocols like OAuth 2.0 and OpenID Connect used in conjunction with the SecureAuth's distributed Microperimeter® authorizer as a local policy decision point at/near the API edge.
- **Data Privacy and Compliance:** Robust encryption and adherence to data privacy and open data regulations.
- **Real-Time Threat Detection:** Advanced analytics and machine learning for continuous monitoring and threat intelligence.
- **User Behavior Analytics:** Detection of anomalies through behavioral analysis of machine learning models created based on users' historical behavior personally and as a community.

By integrating these features, SecureAuth mitigates the risks associated with account takeover, phishing, and credential theft and ensures a secure and seamless user experience by dynamically reducing friction when possible and reacting to increased risk by keeping users safe and in control.

Wrapping It Up: Why a Strong CIAM Strategy is Your Best Defense

Safeguarding customer identities is paramount for maintaining trust and ensuring business continuity. A proper CIAM architecture, incorporating adaptive passwordless multi-factor authentication, threat intelligence, secure API access control, user behavior analytics, and data privacy, provides comprehensive protection against account takeover, phishing, and credential theft. SecureAuth's CIAM solution demonstrates how these components can be effectively integrated to safeguard users and enhance security.

Implementing a robust CIAM architecture is not just a technical necessity but a strategic imperative for businesses aiming to protect their customers and their reputation in the face of evolving cyber threats.

About SecureAuth

With leading Identity and Access Management solutions from SecureAuth, organizations worldwide find it easier than ever to create digital experiences that are as welcoming as they are secure. Our AI-driven Risk Engine helps deliver dynamic – and often invisible – authentication and authorization for users, combined with a data privacy framework that protects their information and ensures their consent.

It all adds up to a virtual handshake at the digital door to your company. Making you more effective than ever at eliminating bad actors or incorrect authorizations. Keeping your employees engaged and productive. And delighting your customers so you can fuel your digital growth. Welcome to Better Identity.

Learn more at SecureAuth.com