frontegg

The CIAM Vendor Guide for Healthcare SaaS Companies

2025

v1.0

Helping healthcare SaaS companies choose a flexible, enterprise-grade CIAM vendor.

Customer Identity and Access Management (CIAM) can be a source of stress for any SaaS company that serves the healthcare industry. Not only do you have to plan for stringent regulations like HIPAA compliance; you have to do so while navigating complex organization structures and stakeholders. But both homegrown and legacy identity management systems often add to this pressure due to the sheer amount of maintenance required to avoid mistakes.

Unfortunately, buyers perusing feature lists on CIAM websites will find significant overlap between vendors. This raises questions – what's special here? Why pay a premium for features that are anything but? And which features are largely the same across the entire marketplace, making them effectively table stakes?

This guide aims to help healthcare SaaS buyers identify truly differentiated CIAM solutions that are built for scale in highly regulated multi-tenant environments.

frontegg

Table of Contents

Organization and Methodology

For this CIAM Guide, we examined features across eight major CIAM providers that we think represent a broad cross-section of the market. We recognize that vendors not included on this list may offer CIAM-related features, but the group we assembled has CIAM as the core of their business.

To create a straightforward mechanism for comparison, we divided CIAM features into three categories indicating the degree of commonality of the feature offer.

Commodity = offered by three or more vendors

Differentiated = only offered by two vendors

Unique = only offered by one vendor

That said, the listed commodity features have great differences in their actual capabilities. For example, some vendors may offer “magic email” but not passkeys for passwordless authentication. Both vendors in this example will receive credit for covering the feature, even if their method of coverage is different. For this reason, it’s critical for CIAM buyers to analyze and verify the details of each feature that matters to them.

Equally important, within a feature category there may be differences in the level of technical skill required to enable, implement, or manage the feature. Some CIAM vendors require coding and configuration changes. Some may even require that an admin at the SaaS provider makes changes for them. Other CIAM systems may be designed for less technical users with visual workflows, checkboxes, and fields to modify user access or roles.

Feature Breakdowns and Comparisons: From Commodity to Unique

Different CIAM vendors use different terms and definitions for common features. In this section, we try to standardize between the detailed feature variations and provide commentary on which features are commoditized, unique, or somewhere in between.

Authentication

Authentication is a foundational part of CIAM. As such, many of the vendors discussed in this section offer similar products.

But does that make authentication a commoditized feature set? The devil is in the details. For instance, most vendors offer passwordless and magic links, but not everyone offers OTPs (one-time-passwords or one-time passcodes).

The moral of the story? Even for apparently commoditized features, there are real differences that can strongly impact your product decision.

Capabilities	Frontegg	AuthO	Stytch	FusionAuth	Clerk	Descope	Amazon Cognito	WorkOS
Standard login	✓	✓	✓	✓	✓	✓	✓	✓
Passwordless	✓	✓	✓	✓	✓	✓	✓	✓
No-Code Customization	✓	✓	✗	✓	✓	✓	✓	✓
M2M Authentication	✓	✓	✓	✓	✗	✓	✓	✓
Hosted IDP	✓	✓	✗	✓	✗	✓	✓	✓
Customizable Workflows	✓	✓	✗	✓	✗	✓	✓	✗
Signup via SMS	✓	✓	✓	✓	✓	✓	✗	✗

Standard login Commodity

The most plain vanilla feature. Every vendor offers standard login but, there are differences in:

- What's supported (OAuth 2.0, SAML, OpenID, and SSO).
- Which features are out-of-the-box or require additional coding or configuration changes.
- How they handle customization, integration, and security.

Engineers should consider how much customization is needed and what level of control is required over security and user experience.

Example #1 Customization: some tools offer pre-built login UIs with no-code configuration, making setup quick but limiting flexibility. Other tools provide fully API-driven authentication, giving developers complete control over the login flow at the cost of more implementation effort.

Example #2 Security and Passwords: some tools focus more on passwordless options like passkeys or magic links. Security policies also widely differ–some platforms allow you to enforce adaptive authentication out-of-the-box, while others require manual configuration.

Passwordless Commodity

Many vendors offer passwordless, but few vendors offer the exact same functionality.

On the surface this is a commodity feature, but with significant differences at the feature and implementation layer. For example, some solutions rely primarily on biometric authentication using native device hardware, while others emphasize adaptive authentication leveraging contextual signals such as geolocation and behavioral analytics.

No-code Customization Commodity

There are different levels of no-code customization.
At the most basic level, some platforms provide drag-and-drop modular blocks, enabling users to visually construct identity flows by assembling pre-defined components. These solutions typically excel at empowering non-technical users to quickly build straightforward use cases, often without significant complexity or customization.

At a more advanced level, certain vendors incorporate natural language processing (NLP) and AI-driven interfaces. These solutions translate plain-text descriptions provided by the user directly into functional workflows or automated processes. This dramatically lowers the barrier to entry by eliminating the need to visually manipulate or understand the underlying structure entirely. Instead, users articulate their intent in everyday language, allowing the AI to interpret, design, and implement the workflow dynamically.
Between these two extremes lies a spectrum of customization capabilities. Some platforms blend visual tools with guided templates, contextual recommendations, or AI-powered suggestions. These intermediate solutions enable deeper customization than basic drag-and-drop approaches but still offer guardrails that prevent errors and streamline development.

Ultimately, the level of no-code customization impacts not just the ease and speed of deployment but also the flexibility, scalability, and complexity of workflows achievable by the end-user.

M2M authentication Commodity

Machine-to-machine communication is essential for many types of apps that integrate with backend services. With the rise of AI agents, the number of M2M application use cases and exposures is set to soar. Within M2M authentication, there are clear differences. Some vendors only support APIs going into their own cloud services. Others support more open protocols. Some support directory capabilities, allowing for better integration with internal systems. Some support mTLS but not JWT. So, again your mileage may vary widely.

Hosted IdP Commodity

An Integrated Developer Platform (aka “sandbox”) is common for CIAM platforms that offer more advanced capabilities. (Note – not to be confused with Identity Provider – IdP) This platform allows for easier testing of changes to CIAM configurations and settings. These environments are mostly the same across providers with slight differentiations in user interface, required knowledge of related services (AWS), and developer focus (React, NextJS, Tailwind).

Customizable Workflows Commodity

Customizable workflows allow for the easy reordering and adding of steps to auth flows and other processes in CIAM management. Some providers offer built-in no-code/low-code workflow builders. Others rely on APIs and SDKs, which offer deep customization and control but require greater developer effort to implement complex workflows. A few platforms focus mainly on enterprise integrations (Directory) or passwordless authentication, offering fewer workflow customization options for general CIAM scenarios.

Signup via SMS Differentiated

This feature simplifies onboarding, reduces friction, and increases conversion rates for users who may not want to register with an email or password. It provides a quick and familiar way to verify identity making it useful for mobile-first users, businesses operating in regions where email adoption is low, and services requiring rapid account creation.

A strong SMS signup feature should include OTP-based verification for security, rate limiting and fraud detection to prevent abuse, and fallback options like email or authenticator apps for users who can’t receive SMS. It should also support global phone number formats, automatic resend limits, and seamless integration with authentication flows to ensure a smooth, secure experience.

Authorization

Authorization is an important differentiator for customers and CIAM vendors. Healthcare SaaS companies that offer flexible and customizable authorization have an edge over those with rigid authorization rules. Most of the CIAM products in this guide were created before authorization became a necessary feature. Retrofitting these capabilities into existing tools proved challenging. Most CIAM solutions in this guide provide basic authorization capabilities like RBAC (role-based access controls) but are not yet advanced in providing granular entitlements.

Capabilities	Frontegg	AuthO	Stytch	FusionAuth	Clerk	Descope	Amazon Cognito	WorkOS
RBAC	✓	✓	✓	✓	✓	✓	✓	✓
ABAC	✓	✓	✗	✗	✗	✓	✗	✗
Subscription-based	✓	✗	✗	✗	✗	✗	✗	✓
API Access Controls	✓	✗	✗	✗	✗	✗	✗	✗
Feature Flags	✓	✗	✗	✗	✗	✗	✗	✓
Trial Management	✓	✗	✗	✗	✗	✗	✗	✓
Fine-grained Authorization	✓	✓	✗	✓	✗	✓	✓	✓

RBAC Commodity

Basic. Check to make sure the RBAC offered has multiple or nested roles, a wide variety of roles, or multiple roles applied to a single user. The ability to assign multiple roles to a single user, to be clear, is offered by multiple vendors. But not all CIAMs offer all of these. CIAM products closely associated with a major cloud (AWS) only offer RBAC that works with services of that cloud, unless you want to do significant custom integration.

ABAC Commodity

Attribute-Based Access Control (ABAC) means controlling users based on characteristics associated with the subject (who is attempting access), the resource (what is being accessed), and the action (what activity is being attempted on said resource). For example:

Subject's title: Software Engineer
Subject's team: RnD
Action: Edit
Action: Download
Resource: Project "x"
Resource: Project "y"

Within the above parameters only team members with matching characteristics are authorized.

In a nutshell, ABAC allows for granular control of usage, feature access, and other attributes based on the individual account rather than the role. ABAC enables more flexibility which is required for more fluid collaborations, inside and outside of an organization. This is a newer concept emergent from the rise of enterprise SaaS and few providers actually offer it.

Subscription-based Differentiated

This capability is closely related to ABAC. It allows SaaS providers to dynamically manage user permissions, access levels, and features based on subscription tiers. It is a core component of enabling DIY authorization for product teams or resellers. A team evaluating subscription management capabilities should look for:

- flexible subscription tiers with granular entitlements
- easy integration with billing systems via APIs and webhooks
- automated handling of upgrades and cancellations
- self-service options for users and administrators
- customizable features that allow for quick modifications to plans, roles, and permissions.

It's likely that more providers will offer various flavors of these in the near future.

API Access Controls Unique

API access controls enable businesses to enforce granular permissions and ensure that users or teams only have access to what they are entitled to at the API level. They are based on roles, subscription levels, or organizational hierarchies.This is essential for API-first SaaS products. When evaluating API access controls, engineers should look for granular RBAC and ABAC to enforce permissions based on user roles, subscription tiers, or organizational hierarchy. This will ensure that access is limited to what's necessary. Secure authentication is essential, with OAuth 2.0, JWT tokens, and scoped API keys that have configurable expiration policies to prevent long-term unauthorized access. Rate limiting and quotas help manage API usage across different user levels.

Feature Flags Unique

Most CIAM vendors do not offer feature flags, which often require code or purpose-built tools. However, moving feature flags into CIAM enables more DIY SaaS management capabilities like tiered rollouts or specific product modifications at the user, account or team level. This allows revenue and product teams to create unique customer packages.

A solid feature flag system in CIAM should let you turn features on and off per user, role, or subscription tier without needing a code deploy, and it should work in real-time so users don't have to log out or refresh to see changes. Some platforms offer granular targeting like progressive rollouts, A/B testing, and location-based access, while others only allow basic enable/disable toggles. Seamless integration with authentication and authorization is table stakes, but not all systems tie feature flags directly to user identities, which can make managing access messy. Audit logs and version control are a must for tracking changes and rolling back mistakes, though not every platform provides built-in logging. Some vendors give

non-technical teams a simple UI to manage flags, while others require API calls or developer intervention for every update. Security also varies–some systems ensure flags aren't exposed in client-side code, while others leave room for potential abuse. And finally, performance matters, since a well-built flag system won't slow down API calls or introduce latency, especially at scale.

Trial Management Differentiated

Trial management ensures users can test a product while maintaining security and preventing abuse. CIAM solutions help by handling authentication, user provisioning, and enforcing access limits. Some providers offer built-in entitlements and automated trial expiration, while others require custom logic or external tools to manage trial access.

The best solutions support flexible trial durations, seamless upgrades, and integrate with billing and CRM systems to track usage and drive conversions. They also include security features like identity verification and domain restrictions help prevent unauthorized trial extensions. More advanced trial management capability allows non-technical teams (revenue, sales, customer success) to control and configure trials, even down to the feature availability level.

Fine-Grained Authorization Unique

Fine-grained authorization controls access to specific actions, data, or resources based on roles, attributes, or policies, rather than broad role-based access alone. This is critical for multi-tenant applications, partner ecosystems, and enterprise environments where users need different levels of access within the same organization. CIAM providers implement fine-grained authorization in different ways. Some offer built-in policy engines that support role, attribute, and hierarchy-based access with API-driven enforcement. Others rely on external policy services or require custom logic to handle complex permissions. Engineers evaluating a CIAM solution should check for support for hierarchical roles, dynamic attribute-based rules, real-time permission evaluation, and integration with external authorization frameworks. Key questions to ask include:

- How are permissions managed at scale?
- Can access rules can be updated dynamically without redeployment?
- Will authorization checks add noticeable latency?

A good system should make policy enforcement transparent, manageable via APIs, and scalable across tenants and complex org structures without requiring constant engineering effort.

Mobile Management

Mobile management is crucial in Customer Identity and Access Management (CIAM) as users increasingly access services via mobile devices, necessitating seamless and secure authentication experiences. Mobile CIAM ensures that users can log in, manage their profiles, and access services securely on their mobile devices. This helps enhance user satisfaction and engagement along with security.

Among CIAM providers there is variation in mobile management capabilities. Some offer comprehensive mobile SDKs which enable developers to integrate authentication, authorization, and user management directly into mobile applications. Others provide robust APIs that, while not mobile-specific, can be adapted for mobile use, requiring additional development effort to optimize for mobile platforms. A few providers lack dedicated mobile support, necessitating custom solutions to bridge the gap between their services and mobile applications. When selecting a CIAM provider, it's essential to assess their mobile management offerings (or lack thereof) to ensure they align with your application's needs and provide a secure, user-friendly mobile experience.

Capabilities	Frontegg	AuthO	Stytch	FusionAuth	Clerk	Descope	Amazon Cognito	WorkOS
Self-service Portal	✗	✗	✗	✗	✗	✓	✓	✓
Passkeys Authentication	✓	✓	✓	✗	✗	✓	✓	✓
Custom login box per tenant	✗	✓	✗	✗	✗	✓	✓	✗
Mobile SDKs	✓	✓	✓	✓	✓	✓	✓	✓
Step-Up Authentication	✓	✓	✓	✓	✗	✓	✓	✓
User Impersonation	✗	✗	✗	✗	✗	✗	✗	✗
Session Management / Idle session	✓	✓	✗	✗	✗	✗	✗	✗

Self-Service Portal

Commodity

A mobile self-service portal should give users direct control over account management. This control includes profile updates, password resets, MFA settings, and role-based access controls, without requiring backend intervention. For engineers, this means designing secure API-driven workflows that sync with authentication and authorization systems, ensuring changes propagate instantly. It should also support JWT or session-based authentication, enforce security policies dynamically, and integrate with SCIM or directory sync for enterprise use cases. Without a well-built self-service portal, routine identity management tasks turn into manual support tickets, increasing operational overhead and reducing scalability.

Passkeys Authentication Commodity

Mobile passkey authentication replaces passwords with biometric login (Face ID, Touch ID) or device-bound cryptographic keys, making logins more secure and reducing friction. Unlike desktop passkeys, mobile implementations need to handle device changes, syncing across multiple devices, and secure storage in iCloud Keychain or Android's Credential Manager. This matters because it removes phishing risks, speeds up authentication, and improves security by keeping credentials tied to physical devices.

A good implementation should support cross-device sign-ins, backup options if a device is lost, and smooth integration with native biometric prompts.

Custom Login Box Per Tenant Commodity

Customizable login boxes per tenant let multi-tenant applications apply unique branding, authentication flows, and security settings for different clients while keeping a shared infrastructure. This is important for B2B SaaS, resellers, and white-label apps that need custom logos, colors, localized text, and authentication options like SSO or MFA per tenant. A good implementation should support tenant-specific UI customization, configurable authentication policies, and per-tenant identity provider settings, all managed through APIs or admin dashboards. This reduces engineering overhead while making it easy to adjust authentication settings dynamically without separate deployments.

Mobile SDKs Commodity

Mobile SDKs play a crucial role in identity for mobile applications. By integrating CIAM-specific SDKs, developers can implement robust authentication mechanisms such as single sign-on (SSO), biometric verification, multi-factor authentication (MFA), and social login capabilities. These SDKs not only streamline the user experience by reducing friction during registration and login processes but also enhance security by efficiently managing identity lifecycles, enforcing access policies, and protecting sensitive user information.

Step-up Authentication Unique

Step-up authentication on mobile requires users to re-verify their identity before performing sensitive actions, such as transferring funds or updating account settings. A solid mobile implementation should support biometrics (Face ID, Touch ID), passkeys, OTPs, and push notifications. It should also include adaptive triggers based on device, geolocation, risk signals, or behavioral analytics. Engineers should focus on low-latency authentication flows that don't disrupt the user experience and secure API integration to enforce step-up verification consistently across mobile and backend services.

User Impersonation Unique

User impersonation on mobile allows admin or support teams to log in as a user to troubleshoot issues or assist with settings. Mobile implementations must ensure session isolation, so impersonation doesn't persist after switching users. Engineers should look for audit logging of all impersonation activity, clear UI indicators for active impersonation, and role-based restrictions to limit access to sensitive data. Secure token handling is critical to prevent impersonation misuse or session leaks.

Session Management / Idle Session Unique

Session management on mobile must handle backgrounding, app switching, and idle timeouts while maintaining security and a smooth user experience. A strong mobile session system should support silent token refreshes to avoid unnecessary logins, biometric reauthentication on wake, and granular idle timeout settings that balance security with usability. Engineers should ensure secure local storage of session tokens and automatic logout or session expiration when risk conditions are detected, such as location changes or repeated failed authentications.

B2C and B2B

B2C and B2B healthcare companies have specific CIAM needs. While this guide was created for B2B SaaS use cases, we will also briefly discuss B2C for those companies that have a dual business model.

B2C B2C capabilities are primarily focused on creating a smooth sign up and login experience for patients. For example, most B2C users are expected to sign up for services themselves, while B2B users are typically invited to a service.

Another big difference is how well a CIAM solution lets businesses customize user roles and permissions at different levels, so teams can manage access in a way that actually makes sense for their structure. The more advanced solutions reduce manual work and keep everything organized, while others may require custom development to achieve the same level of flexibility.

Capabilities	Frontegg	AuthO	Stytch	FusionAuth	Clerk	Descope	Amazon Cognito	WorkOS
B2C Capabilities	✓	✓	✓	✓	✓	✓	✓	✓
Admin Management	✓	✓	✓	✓	✓	✓	✓	✓
Account Hierarchies	✓	✓	✗	✗	✗	✗	✗	✗
Role-level Multi-app control	✓	✗	✗	✗	✗	✗	✗	✗
Login per Application	✓	✓	✗	✗	✗	✗	✗	✗

B2C Capabilities Commodity

B2C is all about reducing friction. How easy is it to login to your application? How easy is it to reset your password? What balance should we strike between upholding security measures for users and getting them into our app as quickly as possible? When evaluating an identity provider you'll want to keep user experience top of mind. Some features to consider include:

- Login branding customization
- A large variety of social login options
- Easy account registration
- Fake account prevention
- Easily reset passwords
- Custom attributes

We discuss these features at length in different areas of this guide, but it's worth noting that these features are commonplace with most identity providers.

Admin Management Commodity

This is a basic B2B feature that enables an admin to manage all the accounts of an organization. Some CIAM platforms handle organization management better than others, especially when it comes to how admins manage all the accounts under a business. The more advanced ones let admins oversee multiple teams, departments, or business units from a single place. This makes it easier to assign roles, adjust permissions, and keep things organized without a ton of manual work.

Some platforms also support multi-tenancy natively, meaning businesses can manage separate customer organizations within the same system. Others require custom development or external tools to handle things like role inheritance, access delegation, or different permission levels across an org.

A few platforms are built for individual user authentication and struggle with large-scale org management. The best ones make it simple for admins to create, manage, and automate organization-wide settings.

Account Hierarchies Differentiated

Account Hierarchies allow admins to transform basic user repositories into intricate, multi-layered organizational structures. This capability is valuable for anyone using partners, resellers, or any type of sub-account. Very few CIAM vendors offer this right now, and it's unlikely to become a common feature because it requires platform changes from the bottom up.

A solid hierarchy system in CIAM should support nested organizations with built-in multi-tenancy, delegated admin controls, role inheritance, scoped API access, automated org provisioning, and per-organization SSO. These features prevent developers from having to build custom workarounds to handle partners, resellers, or multi-level business accounts. It should also keep user data isolated, enforce permissions cleanly, and provide real-time audit logs and webhooks, making it easier to scale complex B2B access without duct tape solutions.

For parent-child capabilities in a CIAM platform, developers should look for built-in support for multi-level organizational hierarchies where parent accounts can create and manage child accounts, delegate admin roles, and enforce policies across sub-organizations. The best systems allow role inheritance, meaning permissions set at the parent level can automatically apply to child accounts while still allowing overrides. Scoped API access should ensure that parent accounts can manage multiple child accounts securely, without exposing data between unrelated entities. Without these features, managing multi-tiered accounts often requires custom workarounds.

Role-Level Multi-app Control Unique

This enables granular control over user roles and permissions within a hierarchical or multi-tenant organizational structure. This capability allows SaaS providers to assign roles and manage access rights at different levels of an organization, ensuring fine-grained access control and streamlined entitlement management.

Instead of a flat, one-size-fits-all role assignment, this approach allows users to have different roles in different organizational contexts–like being an admin for one business unit while only having read-only access to another. This is crucial for SaaS companies serving B2B customers, where businesses often have teams, sub-teams, partners, or resellers that require separate access control. Developers should look for granular role assignments that allow users to have different roles across teams, departments, or organizations without duplicating accounts.

Role inheritance is key for managing permissions efficiently, letting parent roles pass down access rules while allowing overrides when needed. A good system should support dynamic role changes via APIs, so roles can be updated programmatically as org structures evolve. Scoped access control ensures users only see and interact with what their role allows, preventing data leaks across tenants.

Login Per Application Differentiated

Login per application in CIAM enables users to authenticate within the specific context of their organization rather than through a generic login flow. When a user logs in they see branding, security policies, and access rules that are specific to their organization. This capability is particularly valuable for businesses with resellers, partners, or multi-tenant customers, where a single CIAM system needs to support multiple independent organizations while maintaining data separation and enforcing organization-specific authentication rules. Without this, businesses often have to build custom logic to route users to the correct identity provider or enforce different security policies per organization, adding complexity and potential security gaps.

Developers should look for organization-aware authentication, where users are automatically directed to the correct login experience based on their email domain, subdomain, or unique org identifier. Flexible authentication methods per organization, including custom SSO setups and different MFA policies, are helpful to businesses managing enterprise customers with varying security needs. Scoped session management ensures that logging into one organization doesn't grant unintended access to another, and custom branding per org provides a seamless, user-friendly experience. A strong system should also allow for tenant-aware APIs, so developers can manage org-specific authentication settings dynamically without hardcoding different login flows.

Advanced Security

The growing threat of ransomware, business email compromise (BEC), and other advanced cyberattacks has put a spotlight on advanced security capabilities. Multi-factor authentication (MFA), organizational-level policies, and customizable step-up authentication allow organizations to enforce tailored and robust security protocols. These capabilities ensure compliance with evolving regulatory standards while addressing the increasing sophistication of threats.

Capabilities	Frontegg	AuthO	Stytch	FusionAuth	Clerk	Descope	Amazon Cognito	WorkOS
Risk/fraud engines	✓	✓	✓	✓	✗	✓	✓	✓
Security Dashboards	✓	✓	✓	✗	✗	✗	✗	✓
Adaptive MFA	✓	✓	✗	✓	✗	✓	✓	✗
Customizable Step Up	✓	✓	✗	✓	✗	✓	✓	✓
Logs Streaming	✓	✓	✓	✓	✗	✓	✓	✓
Consent Management	✓	✗	✗	✗	✗	✗	✗	✗
Sessions Management	✓	✓	✓	✓	✗	✗	✗	✓
Device Fingerprinting	✓	✓	✓	✓	✓	✓	✓	✓

Risk + Fraud Engines Commodity

CIAM solutions must include risk and fraud engines because every SaaS is under attack. A vendor's failure to provide these features is likely a non-starter. Risk and fraud engines are essential for preventing unauthorized access, credential stuffing, brute-force attacks, and account takeovers in any SaaS platform. The best CIAM solutions have built-in real-time threat detection that monitors login behavior, device fingerprints, IP reputation, and geolocation anomalies to identify suspicious activity. Some providers offer adaptive risk scoring, dynamically adjusting authentication requirements–such as triggering MFA or blocking access–based on risk levels. Others rely on third-party fraud detection tools, requiring additional integration effort and adding complexity to security workflows. Without a strong risk engine, SaaS platforms are exposed to automated bot attacks, phishing exploits, and malicious account takeovers, making this a non-negotiable feature.

Key factors to evaluate are event-driven risk analysis, low-latency decision-making, and API-driven security responses that allow for real-time enforcement of fraud rules. A strong system should support custom risk policies, where developers can define how the platform reacts to specific threats, such as requiring step-up authentication or flagging accounts for review.

Security Dashboards Commodity

Dashboards make it easier for application security teams to quickly assess security status and identify anomalous signals. Security dashboards provide application security teams with real-time visibility into threats and system vulnerabilities, allowing them to quickly assess risks and respond to potential attacks. A well-designed dashboard should categorize security events, distinguishing between mitigated and unmitigated incidents, so teams can prioritize urgent threats without getting overwhelmed by routine logs.

Centralizing this data streamlines threat monitoring, anomaly detection, and incident response, ensuring that security teams can take proactive action before issues escalate. This is new territory for CIAM so we expect more CIAM providers to show up with these capabilities in the near future.

Adaptive MFA Commodity

With SIM-swapping, email takeovers, and even deep fakes becoming more common, creating multi-factor authentication (MFA) that adapts to increased security risks is important for SaaS platforms. Adaptive MFA becomes even more critical as artificial intelligence makes spear-phishing easier to execute. By evaluating contextual factors such as login and user behavior, device information, geolocation, IP reputation – even typing cadence – adaptive MFA can intelligently determine the necessity and method of additional authentication steps. This approach not only enhances security but also maintains a seamless user experience by applying stricter measures only when suspicious activity is detected.

Different Customer Identity and Access Management (CIAM) providers implement adaptive MFA with varying capabilities. Some platforms offer comprehensive adaptive MFA solutions that assess multiple risk signals–such as new device usage, impossible travel scenarios, and untrusted IP addresses–to calculate an overall risk score during each login attempt. If a high risk is detected, users are prompted for additional verification, ensuring that security measures are proportionate to the threat level.

Other providers offer more basic MFA implementations without adaptive features, requiring uniform authentication steps for all users regardless of context. The absence of adaptability can lead to either insufficient security or unnecessary friction for legitimate users. Therefore, when selecting a CIAM solution, consider the sophistication of its adaptive MFA capabilities to effectively balance security needs with user convenience.

Customizable Step Up Commodity

Customizable step-ups enable organizations to increase requirements for more sensitive application areas or system responses to anomalous conditions. This is related to Adaptive-MFA. A strong step-up authentication system should allow customized security triggers, so additional verification is only required when users perform sensitive actions, like accessing financial data or changing account settings. It should support multiple authentication methods, such as one-time passcodes, biometrics, or hardware keys, ensuring flexibility based on risk level. Context-aware rules should adjust authentication dynamically, increasing security for logins from unfamiliar locations or new devices while keeping the process seamless

for trusted users. The best systems strike a balance between strong protection and ease of use, reducing unnecessary friction while securing critical areas of an application or the most important business logic. Ideally, teams should be able to define and change their own step-up criteria for an application or even an organization, based on business requirements and evident risks.

Logs Streaming Commodity

A strong log streaming system should provide real-time access to security events, allowing threat detection and fraud prevention tools to act immediately on suspicious behavior. Continuous data flow ensures that authentication attempts, failed logins, step-up challenges, and other key security events are instantly available, rather than being processed in delayed batches. Structured, high-resolution event data is crucial for AI-based detection engines to recognize subtle patterns and anomalies, such as unusual login attempts, credential stuffing, or account takeovers. The best systems allow for customizable event filtering, so only relevant security data is streamed, preventing unnecessary noise while keeping systems responsive. Seamless integration with external monitoring and SIEM tools ensures that logs are actionable, feeding into security workflows without requiring constant manual intervention. Ideally, too, streaming data can enter into security dashboards in real time, giving application security and security monitoring teams immediate observability of risky behaviors.

Consent Management Unique

With new laws around the globe mandating tighter compliance around user notification and consent (particularly in tightly regulated industries like health care and financial services), managing consent at scale is now a top checklist item for compliance and risk teams. Consent management needs to go beyond individual user preferences and address organization-wide policies that define how data can be collected, shared, and processed across teams. Companies should be able to configure consent settings at both the user and organizational level, allowing admins to enforce compliance rules while still giving individual users control over their personal data. Granular consent tracking ensures that specific permissions—such as marketing preferences, data sharing agreements, or security disclosures—are logged and updated dynamically as regulations change. Versioning and auditability allow businesses to maintain a record of past consent agreements for legal and compliance reviews. For international SaaS platforms, regional compliance settings should enable different consent requirements based on jurisdiction, ensuring adherence to GDPR, CCPA, and other global regulations.

Session Management Commodity

Session management should provide real-time tracking and control over user sessions to prevent hijacking, unauthorized access, and abuse. Adaptive policies should adjust session behavior based on risk signals like device, browser, IP, and location anomalies. Idle timeouts, forced reauthentication, and session expiration rules help reduce exposure to attacks.

To prevent session hijacking, device binding and token validation ensure stolen tokens can't be reused on another device. Refresh token rotation and automatic revocation block attackers from maintaining access, while session isolation lets users monitor and terminate unauthorized sessions. Real-time security logging provides visibility into session activity, allowing quick responses to threats. A strong system enforces tight security without disrupting legitimate users, keeping access both seamless and safe.

Device Fingerprinting Commodity

Device fingerprinting captures unique attributes of a user's device–such as browser version, OS, IP address, screen resolution, and installed plugins–to create a persistent identifier that helps detect unauthorized access. It plays a key role in session security and risk assessment. If a fingerprint doesn't match a previously trusted device, additional security measures–such as multi-factor authentication (MFA) or step-up authentication–can be triggered to verify the user's identity.

While device fingerprinting is a useful baseline security feature, it's widely available and should not be a major differentiator when selecting a CIAM provider. Most platforms offer some form of fingerprinting, but more advanced solutions go beyond simple device snapshots and incorporate behavioral analytics, anomaly detection, and adaptive security policies that analyze how users interact with the system.

A stronger approach integrates continuous authentication rather than relying solely on a static fingerprint, which can be bypassed by attackers using virtual machines, device spoofing, or session hijacking. The real value lies in how fingerprinting is used alongside other risk signals to strengthen security without adding unnecessary friction for legitimate users.

Enterprise Readiness

Enterprise readiness features like SSO, SCIM, and audit logs are standard across CIAM solutions, but their implementation varies in depth and flexibility. Some platforms support a full range of SSO protocols (SAML, OAuth, OpenID Connect) with easy configuration, while others require more complex setup or lack full protocol coverage, making integration harder. SCIM provisioning also differs–some providers offer deep customization options for user lifecycle management, while others provide only basic provisioning and deprovisioning that may require additional scripting or API work. Audit logs are another key area where differences emerge; the best platforms offer real-time, searchable logs with fine-grained event tracking, while others provide delayed or limited logging, making security monitoring and compliance more challenging.

For developers, the real concern is how easily these features integrate with existing enterprise infrastructure and how much work is needed to get them production-ready. Some CIAMs provide fully managed SSO with just a few configuration steps, while others require custom integration efforts, especially when dealing with complex enterprise setups. SCIM support should be fully automated and configurable, rather than requiring manual API calls to manage users. Audit logs should be streamed in real time and accessible via APIs, enabling seamless monitoring and response workflows. While these features are table stakes, the difference lies in how much engineering effort is needed to make them work smoothly at scale.

Capabilities	Frontegg	AuthO	Stytch	FusionAuth	Clerk	Descope	Amazon Cognito	WorkOS
SSO	✓	✓	✓	✓	✓	✓	✓	✓
SCIM	✓	✓	✓	✓	✗	✓	✓	✓
Audit Logs	✓	✓	✓	✗	✗	✓	✓	✓

SSO Commodity

SSO is standard across CIAM platforms, but things like protocol support and ease of setup vary widely. Some solutions support SAML, OAuth, and OpenID Connect with low-code configuration, making it easy for non-technical users to set up. Others require developer involvement for integration, especially when dealing with enterprise IdPs or custom authentication flows. Some platforms offer intuitive admin panels for managing SSO settings, while others rely heavily on API-based configurations. The difference isn't just whether SSO is supported – it's how easily it integrates and who can manage it.

SCIM Commodity

SCIM is different from SSO because it automates user provisioning and deprovisioning. This ensures that when a user is added, updated, or removed in one system, those changes sync across all connected applications. In CIAM, SCIM support varies–some platforms offer full SCIM 2.0 compliance with customizable attribute mapping and automated sync, making it easy to integrate with enterprise identity providers. Others provide only basic user provisioning, requiring extra API work to handle role assignments, group management, or real-time updates. Some systems also lack deprovisioning support, which means offboarded users may retain access longer than they should, creating security risks. The best SCIM implementations are fully API-driven, support push and pull synchronization, and require minimal manual intervention.

Audit Logs Commodity

Audit logs can come in various flavors including format, frequency and different paid tiers for how long your logs will be maintained. While the functionalities are mostly the same, the pricing may not be and can create a “gotcha” for fast-growing SaaS players. Making audit logs expensive or hard to access can be particularly problematic when serious security breaches happen. Expensive audit log export and storage also may result in users and their organizations failing to readily perceive or measure value from usage of a SaaS tool. Audit logs should be exportable in common formats like JSON or CSV and consumable via APIs for dashboarding systems, SIEM, auditing platforms and other relevant monitoring and oversight components. Failure to offer audit log export will make full compliance with the new crop of government regulations around resilience and security a significant challenge.

Management & Analytics

While user management is a standard feature across CIAM platforms, the availability of usage analytics and behavioral insights varies widely. Some solutions provide detailed organizational signals that track user engagement, feature adoption, and login behavior. This helps businesses identify customer health trends and internal champions who drive product adoption. These analytics are key for product-led growth, churn prevention, and upselling opportunities. The difference between CIAM solutions isn't just in managing users–it's in how well they help organizations understand and act on user behavior.

Capabilities	Frontegg	AuthO	Stytch	FusionAuth	Clerk	Descope	Amazon Cognito	WorkOS
User Management	✓	✓	✓	✓	✓	✓	✓	✓
Usage dashboards	✓	✓	✓	✗	✗	✗	✗	✗
User export	✗	✓	✗	✗	✗	✗	✓	✗

User Management Commodity

Every vendor offers some basic level of this feature, which is more or less commoditized. That said, user management in CIAM varies widely in capability and ease of use, as well as technical requirements (code or config vs. DIY). These affect how businesses handle registration, authentication, and access control. Some platforms offer fully customizable registration flows with built-in MFA and flexible social login options, while others have basic authentication with limited identity provider support. Consent management is another key difference–some solutions provide built-in privacy controls for GDPR and CCPA compliance (see our section on this), while others require custom development to meet regulatory needs. User profile management also ranges from rich, customizable attributes and progressive profiling to simple, static user records with little flexibility. The right choice depends on whether an organization needs basic identity handling or deeper control over user data and access.

Usage Dashboards Commodity

Dashboards seem obvious – every SaaS platform has them for other use cases but not for user management. Surprisingly, they are not widely available outside of a few vendors. A strong usage dashboard should include key engagement metrics, like active vs. inactive users, authentication success rates, and step-up authentication frequency, enabling teams to continuously refine access policies based on actual usage patterns. It should offer sophisticated real-time anomaly detection, immediately flagging suspicious activities such as unusual login locations, potential credential stuffing attempts, or patterns of failed authentication attempts. Multi-tenant visibility is especially valuable to B2B SaaS providers, allowing organizations to monitor authentication trends across different customer accounts and identify account-

specific security concerns. Finally, effective dashboards must be both customizable and API-accessible, ensuring security teams can extract relevant insights programmatically without being constrained by pre-built views. Without these integrated capabilities, organizations must resort to manually assembling identity analytics from disparate sources, significantly hampering both security monitoring effectiveness and user experience optimization efforts.

User Export Commodity

User Export refers to the capability within an identity management platform to extract user-related data–such as profile attributes, authentication credentials (hashed or metadata only), permissions, group memberships, and event logs–into standardized formats like CSV, JSON, or via RESTful APIs.
For engineers, robust user export features are essential for tasks such as migrating user databases between systems, debugging authentication issues, performing compliance audits, or integrating user data with external analytics platforms. Key technical aspects to look for include support for secure and automated exports (via API or scheduled jobs), selective data exports through advanced filtering criteria, comprehensive logging for audit purposes, and efficient handling of large data sets without performance degradation. As more companies move towards owning their own data fully, this becomes a more important feature.

Advanced Self-Service

Customers can use the capabilities in this section to add additional CIAM features and adjust the end user experience. By offering advanced self-service, CIAM vendors put the power in the customer's hands to manage CIAM requests. Translation? No more waiting for responses from support teams.

Self-service in CIAM allows users to manage their own accounts, update profiles, configure security settings, and request access without relying on support teams. Some platforms offer full control over organization management, SCIM setup, and security policies, while others lack even basic tools like user invitations or M2M token management. The difference comes down to how much manual work is required–without strong self-service, engineering teams end up managing routine CIAM tasks that should be automated. A complete self-service system should let non-technical users, partners, and ad-hoc teams customize their experience, including adjusting login flows, setting up security policies like MFA step-ups, and modifying branding elements such as the look and feel of authentication pages. The best platforms provide intuitive admin tools and API access, making it easy to scale user management while allowing business users to configure authentication and security settings independently.

Capabilities	Frontegg	AuthO	Stytch	FusionAuth	Clerk	Descope	Amazon Cognito	WorkOS
User Management	✓	✓	✗	✓	✓	✗	✓	✗
Usage dashboards	✓	✓	✗	✗	✗	✗	✓	✗
User export	✓	✗	✗	✗	✗	✗	✗	✗
Usage dashboards	✓	✗	✗	✗	✗	✗	✗	✗
User export	✓	✗	✗	✗	✗	✗	✗	✗

Profile Management Commodity

Profile management in CIAM lets users create, update, and manage their personal data, security settings, and preferences. It's important for both user experience and security, allowing people to change passwords, enable MFA, and control privacy settings. For businesses, good profile management ensures data consistency, compliance with regulations like GDPR, and better user engagement. A strong system should have easy-to-use self-service options, customizable fields, API access for automation, and security features like audit logs and adaptive MFA.

Different CIAM providers handle profile management with varying levels of flexibility and depth. Some offer simple, pre-built user profile systems that are easy to integrate but limited in customization. Others provide fully API-driven solutions, giving developers control over fields, permissions, and external integrations.

Some focus on passwordless authentication, embedding profile updates into authentication flows, while others emphasize enterprise-grade features like directory sync and role-based access. A handful of CIAM providers also provide the ability for end-customers to change profile settings themselves via self-service, often with no coding skills required. Choosing the right provider depends on whether the priority is ease of use, customization, security, or enterprise scalability.

User Invitations Commodity

User invitations are an essential feature in CIAM for multi-tenant SaaS platforms. They simplify the process of onboarding new users while e Additionally, certain providers offer visual workflows and embeddable widgets to facilitate user onboarding and self-service capabilities, enhancing the overall user experience.

Organization Management Unique

This is similar to the organizational management we discussed in the B2B section. The key difference is that customers are empowered to set up organizational management themselves. Broadly, organization management in CIAM platforms refers to how user accounts and permissions are structured, controlled, and managed within groups or organizational units. This feature allows admins to set and enforce access rules, roles, and policies consistently across multiple users or teams. It matters because effective organization management simplifies user administration, ensures security through controlled access, and helps maintain compliance, especially in multi-tenant or complex organizational environments.

Key attributes of a good system include support for hierarchical groups or sub-organizations, centralized role-based access controls, flexible policy enforcement, and integration with existing identity systems (like SSO or directory sync). Among the CIAM providers reviewed, some systems offer full support for nested groups, dynamic role assignments, and API-driven management, making them suitable for larger or complex organizations. Others provide only basic user-group functionality, without hierarchical structures or extensive policy control, which may be sufficient for simpler use cases but challenging for enterprises or multi-tenant setups. Developers should verify whether the chosen CIAM solution offers adequate flexibility and granularity to manage their organizational structures effectively.

SSO & SCIM Configuration Unique

System for Cross-domain Identity Management (SCIM) and Single Sign-On (SSO) are protocols that facilitate automated user provisioning and centralized authentication across multiple platforms. SCIM standardizes the exchange of user identity information, enabling automated creation, updating, and deletion of user accounts between identity providers (IdPs) and service providers. SSO allows users to authenticate once and gain access to multiple applications without repeated logins. Integrating SCIM with SSO ensures that user identities and access rights are consistently managed across systems, enhancing security and administrative efficiency.

A well-implemented SCIM and SSO configuration should support comprehensive CRUD (Create, Read, Update, Delete) operations for user and group management, adhere strictly to SCIM 2.0 protocols, and provide clear documentation for integration. Among the CIAM providers examined, some offer detailed guides on configuring SCIM with various IdPs, emphasizing the importance of matching user attributes and maintaining synchronization. Others provide SCIM management APIs and highlight the necessity of disabling conflicting features like Just-In-Time (JIT) provisioning to prevent attribute overwrites. Additionally, certain providers focus on troubleshooting SCIM provisioning and tenant-specific SSO configurations, addressing common errors related to attribute mappings and data synchronization. These differences underscore the importance of thorough documentation and adherence to standards in implementing SCIM and SSO configurations.

Security Configuration Unique

Allowing users and sub-organizations to manage their own security configurations, workflows and policies enables better security hygiene. But not all CIAMs are made alike here. A well-designed security configuration system should offer intuitive interfaces for setting up and managing security features, comprehensive documentation to guide administrators, and flexibility to adapt to various security requirements. Among the CIAM providers examined, differences in ease of security configuration setup are notable. Some providers offer user-friendly consoles with step-by-step guides, allowing administrators to configure security settings like data encryption and authentication protocols efficiently. Others may require more manual setup through command-line interfaces or custom scripting, which could increase the complexity and potential for misconfiguration. Additionally, the availability of pre-defined security templates and integration with existing security tools varies among providers, impacting the overall ease of use for setting up security configurations.

Conclusion: Know what features are worth the price

The CIAM landscape in 2025 is clearly split between commoditized features and differentiated capabilities. SaaS companies who serve enterprise healthcare organizations often require differentiated and advanced features. Multi-tenancy, self-service, and intricate roles and permissions are essential.

Several key insights emerge from this analysis:

First, buyers should be wary of paying premium prices for commodity features. Basic authentication, standard login, and elementary RBAC are table stakes and should be evaluated primarily on ease of implementation.

Second, the future of CIAM points toward more sophisticated B2B capabilities, advanced entitlements management, and granular security controls. SaaS platforms that anticipate growth into multi-tenant environments, channel sales, or regulated industries should carefully evaluate vendors' capabilities in these areas, as retrofitting such functionality later can be challenging and costly.

Third, the shift toward self-service and DIY management of CIAM features is accelerating. Vendors that enable non-technical teams to manage entitlements, security policies, and user access without engineering intervention are better positioned to support modern SaaS operations.

Finally, buyers should align their vendor selection not just with current requirements but with their product's strategic direction. A vendor's feature roadmap and target market orientation can be strong indicators of their ability to support future needs, particularly in areas like API access controls, advanced B2B capabilities, and machine-to-machine authentication.

As the CIAM market continues to evolve, the gap between basic providers and those offering advanced capabilities will likely widen. Forward-thinking buyers should consider not just the features they need today but also the capabilities their SaaS platforms will require to thrive in an increasingly complex and demanding marketplace.

We tried to lay it all out in one place to help you think through the process of selecting a CIAM. It's a serious decision. Choose wisely and carefully.

References

Frontegg Documentation: https://developers.frontegg.com/guides/getting-started/home
Auth0 Documentation: https://auth0.com/docs
Stytch Documentation: https://stytch.com/docs/
FusionAuth Documentation: https://fusionauth.io/docs/
Clerk Documentation: https://clerk.com/docs
Descope Documentation: https://docs.descope.com/
Amazon Cognito Documentation: https://docs.aws.amazon.com/cognito/index.html
WorkOS Documentation: https://workos.com/docs/

Accessed January 2025. Send corrections and updates to unsanctionedguide@frontegg.com.