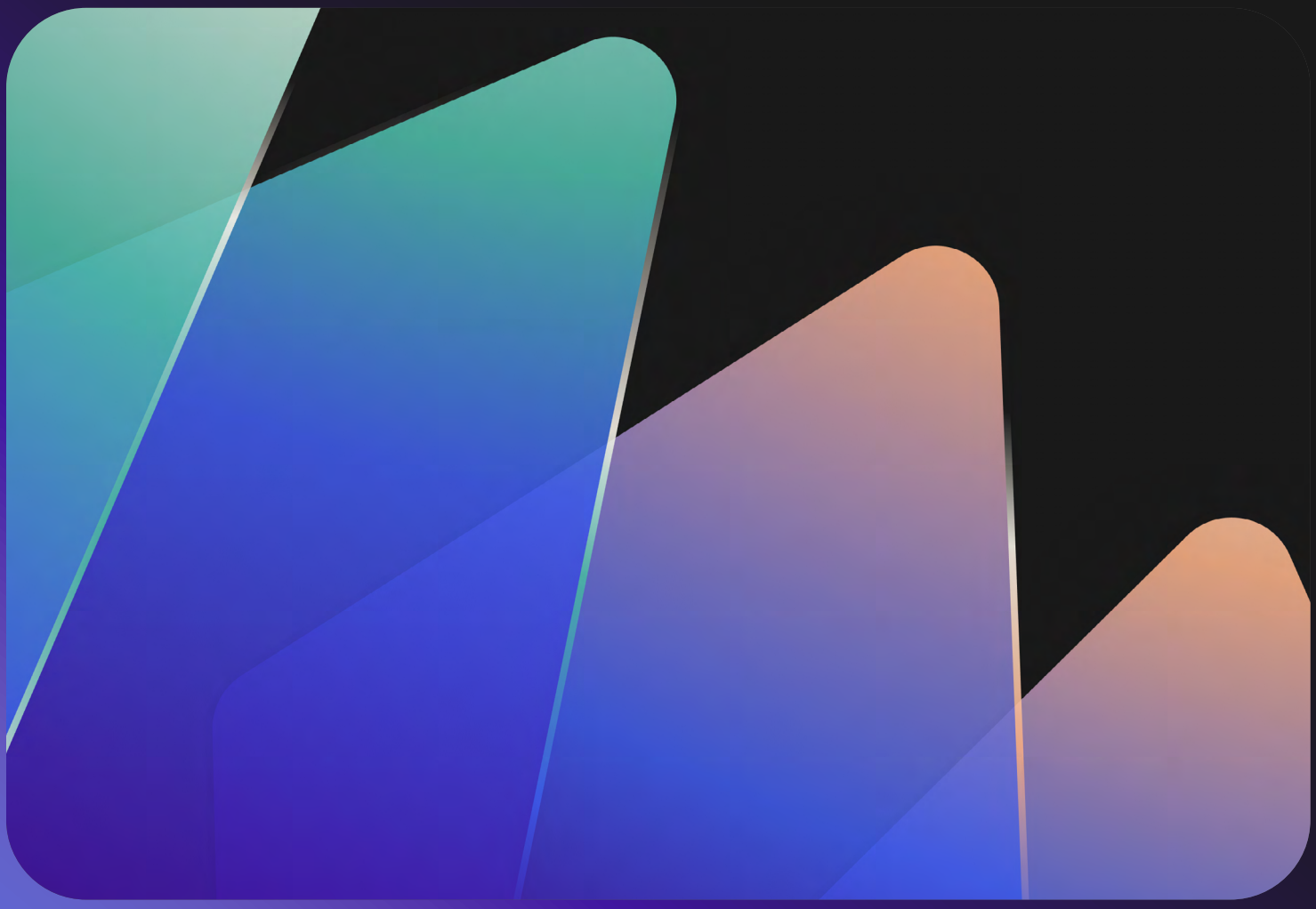
E-book

Why Auth0 by Okta?

Learn why companies just like yours choose the leading independent Identity partner



okta

Auth0 by Okta

Introduction

No longer an afterthought or commoditized component, Customer Identity and Access Management (CIAM) is now rightfully regarded as a way to catalyze growth, shorten time-to-market, achieve regulatory compliance, and responsibly acquire valuable customer data.

But recognizing the importance of Customer Identity and making meaningful progress on implementing CIAM functionality are (clearly) two very different things.

Whether you ultimately build an Identity stack in house or choose instead to incorporate a cloud-based CIAM solution into your applications, our genuine hope is that you make an informed decision that's best for your users.

In this document, we'll show that:

- There's much, much more to Identity than almost all technology pros realize
- Outside of the most basic scenarios (e.g., a simple, internal POC), integrating a third-party CIAM solution into your app or service is faster, more cost-effective for the organization, and results in a more secure, stable, and future-proof Identity stack than building something yourself
- There are many reasons why organizations large and small, in B2C and B2B, choose — and love — Auth0 for their Customer Identity needs

Customer Identity crash course: Five things you need to know

Many IT and development professionals look at Customer Identity and, seeing a login box and API, conclude that building a solution requires little more than a UI, some API calls, and a backend credential database.

Sounds simple enough, right?

Unfortunately, this perception is very wrong — and it has led many a development team to drastically underestimate the time, effort, and expertise needed to build a real-world-ready Customer Identity implementation.

So before you inadvertently overcommit to a product roadmap, here are five important pieces of context on Identity.

#1

Customer Identity is sneakily complex, constantly evolving, and under attack

In Identity terms, four essential features of an effective CIAM solution are:

- **User registration (identification)**, to create the record that makes everything else possible
- **Proper authentication**, to ensure that the users logging into accounts are who they say they are, using one or more factors to do so
- **Effective authorization**, to help organizations provide a user with the appropriate level of access to resources or applications
- **Comprehensive Identity management**, to enable customers and administrators to make updates and changes to users' data and access

But — just as describing a car as a combination of engine, drivetrain, wheels, and steering mechanism is woefully insufficient at capturing what you can do with one — simply summarizing these Identity elements doesn't come close to telling the CIAM story.

In fact, as many organizations have discovered, while Identity can seem conceptually straightforward, it very quickly becomes surprisingly complex.

Regulations impose strict requirements

Identity as a domain is governed by an increasing — and increasingly complex — array of data regulations (e.g., HIPAA in healthcare, GLBA in

finance, GDPR in the EU, LGPD in Brazil, CCPA/CRPA in California, etc.). Among other things, these regulations typically require you to:

- **Implement effective safeguards** to protect credentials, Personally Identifiable Information (PII), Protected Health Information (PHI), and other personal and sensitive data highly valued by cybercriminals
- **Put users in control of their own data** — how it's used, by whom, for what — through mechanisms that allow them to provide and revoke consent across digital touchpoints and to take their data with them if they choose to end a relationship with a service provider
- **Interoperate** within industry (e.g., healthcare, finance) and Identity (e.g., to enable social logins) ecosystems

Identity standards change and grow

Authentication and authorization standards are open specifications and protocols that provide guidance on how to:

- Design IAM systems to manage Identity
- Move personal data securely
- Decide who can access resources

As is the case with many standards, those relating to Identity are constantly evolving — and expectations are that your apps will keep pace.

For example, passkeys — FIDO credentials that are discoverable by browsers or housed within native applications to enable — provide a highly secure and very convenient authentication experience. They're now widely supported by Google, Apple, Microsoft, and password managers, and customers will come to demand them as an authentication option.

Identity is under attack

Securing Customer Identity should be a top-tier priority for any application or service provider, for the simple reason that people other than legitimate users want access to whatever's behind your login box — and these malicious actors are willing to invest considerable effort to get what they want.

The State of Secure Identity Report 2023 demonstrates that signup fraud, credential stuffing, and MFA bypass are all everyday threats that must be managed by practically every organization with an Internet-facing login box or API. From January 1, 2023 through June 30, 2023:

13.9% of attempted account registrations met the criteria of a signup attack, in which malicious users create fraudulent accounts

24.3% of login attempts overall met the criteria of credential stuffing, in which threat actors pursue account takeovers by trying compromised credentials

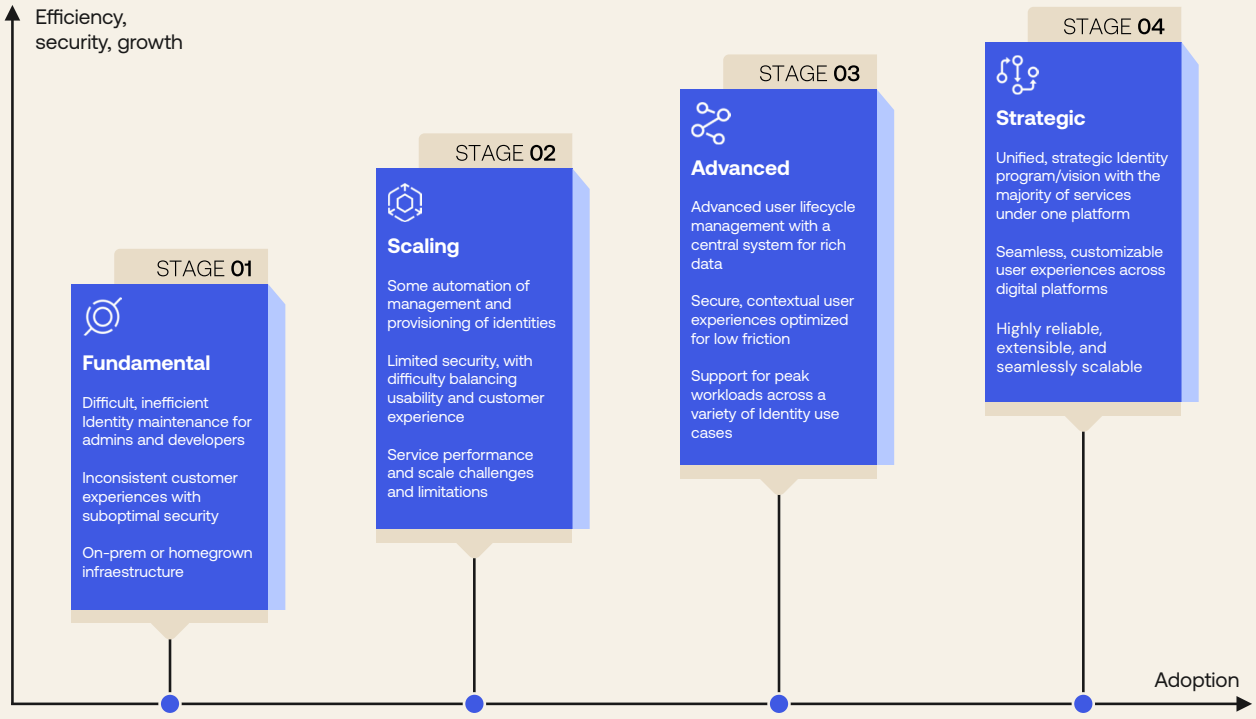
12.7% of MFA attempts were associated with MFA bypass attempts

#2

Implementing CIAM is a journey

CIAM is too large of a domain to tackle all at once. Most companies start with the bare-bones basics needed to win initial customers and then gradually add features over time.

While every organization's journey is unique, deep conversations with thousands of our customers reveal a pattern consisting of four stages of maturation.



By understanding where you are today and where you could be in the future, you'll position your business to plan and deliver an Identity roadmap that enables growth, addresses security, and meets ever-growing customer expectations.

#3

Identity has many stakeholders

CIAM often makes its first appearance as a requirement on a product roadmap, because it can rightfully be regarded as a feature of a larger application technology stack.

This perception isn't wrong, just incomplete. For example:

- Because CIAM sits at the heart of customer-facing systems — influencing acquisition, conversion, and retention efforts, while enabling compliant collection of customer data — sales, marketing, revenue, and customer experience leaders all have a stake.
- At the same time, CIAM has a direct impact on security and privacy, putting it squarely in the sights of CISOs, CIOs, and governance and compliance officers.
- And — fundamentally — CIAM is a set of technology capabilities, causing it to fall under IT organizations, or even CTOs (when properly regarded as an enabler of digital transformation).

It's imperative to find the right balance between user experience and system security. In the context of desired use cases, customer types, data types, and industry-specific risks, leaders across these functions should work together to develop a CIAM plan that satisfies all business needs.

Plus, there's another very important stakeholder group: **your customers ...**

#4

Different customers want different things

Traditionally, CIAM was primarily a tool for managing business-to-consumer (B2C) relationships, but it's also heavily used in the business-to-business (B2B) world.

Minimizing friction for consumers

In an Identity context, "friction" refers to anything that slows down a person's interactions with your service. These interactions may include (but are not limited to) a user:

- Signing up for your service
- Logging in to their existing account
- Updating their information and preferences
- Recovering lost account data
- Checking out (i.e., completing a purchase)

While some amount of friction during these interactions is necessary — both to establish trust and to provide security controls — the more friction involved in an interaction, the greater the user's frustration, the lower your conversion rates, and the less revenue you get over both the short and long term.

Conversely, a poor experience can drive customers to competitors.

An effective CIAM implementation enables you to offer highly personalized promotions and recommendations that drive additional revenue and create more value for your customers. At the same time, it should act as a universal lubricant that minimizes the friction your customers experience when engaging with your digital channels.

Friction is revenue's enemy

Okta's Customer Identity Trends Report revealed that **nearly 60% of consumers** would be more likely to spend money when services offered "a simple, secure, and frictionless login process."

Empowering business customers

Countless organizations rely on software-as-a-service (SaaS) applications. In many cases, different users within each organization need different levels of access to different resources, and creating a convenient and secure experience requires precisely managing Identity and access privileges.

For a B2B SaaS provider, administering this multitude of identities within each customer, across the entire customer base, is complex.

CIAM provides the answer, by empowering B2B SaaS customers to self-manage Identity — creating a highly customized experience that aligns with their unique needs.

And the easier it is to self-manage, the better: the Businesses at Work Report 2023 revealed that the average Okta customer uses 89 different apps — so every organization, large or small, will value well-engineered Identity functionality.

Unlocking enterprise opportunities with Identity

Going upmarket is a frequent goal for B2B SaaS vendors, but it isn't easy. In addition to ensuring your core features meet the needs of enterprise buyers, you also have to satisfy a long list of additional requirements in other areas — including Identity.

While SMB customer needs may have been met with fairly straightforward authentication, authorization, and Identity management features, enterprise decision-makers expect much, much more.

#5

Identity can force trade-offs between user experiences, security, and privacy

Today's companies must enable their customers to engage with their apps or services at any time, from any device, in a secure and safe manner. At the same time, companies must also ensure that these engagements are convenient and consistent, across the full range of digital channels, to keep pace with the best experiences users encounter elsewhere.

As a result, the designers, developers, and IT professionals who build digital services can encounter tension between securing information and protecting private data while also enabling convenient user experiences and providing the organization with valuable insights.

Older Identity technologies and home-built efforts often force a compromise between these priorities, but modern solutions can largely mitigate potential trade-offs — or, at worst, give you much greater control over them.

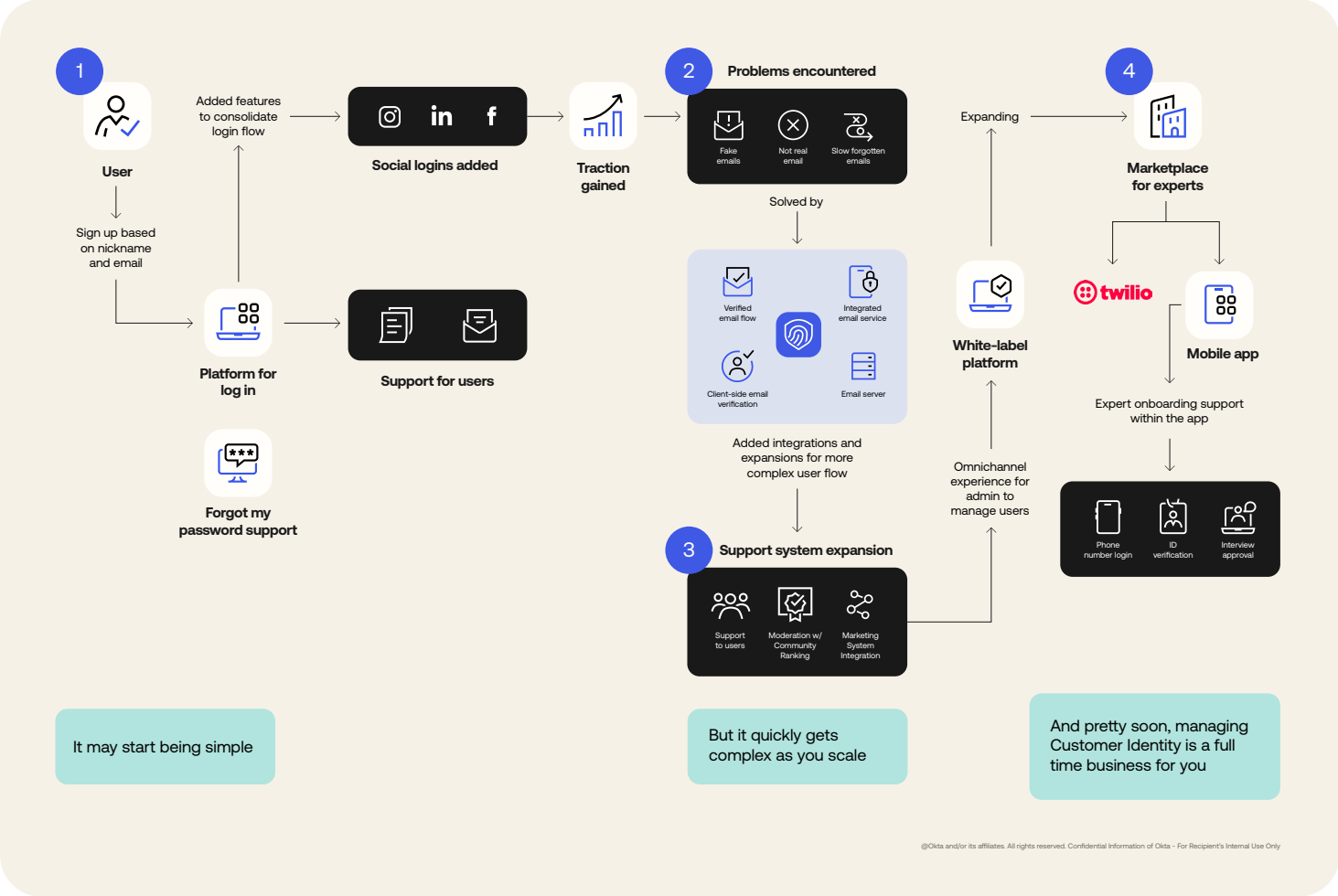
The age-old question — build or buy?

It should be pretty clear by now that building effective and efficient Identity implementations requires considerable expertise. Plus, once built, Identity capabilities need to be maintained and extended — which introduces an added development burden that can easily be overlooked during initial project planning.

This whitepaper explores the build-versus-buy decision in detail — including a total cost of ownership (TCO) comparison and case studies — but we'll touch on a few important considerations, below.

POC != product

There's a big difference between getting some basic login functionality working and having a stable, scalable, and prime-time-ready Identity infrastructure in place.



For example, a proof-of-concept web app might rely entirely on Facebook for authentication (via Single Sign-On / Social Login) and have an all-or-nothing authorization policy.

In this scenario, your app performs a simple check: If a user isn't currently logged in to Facebook in the current browser, you direct them to do so. Once authenticated, all users can access everything in your app.

However, while that might make for a useful demo, it's unlikely that such a simple implementation would meet the needs of your users, organization, industry, or compliance standards. In real life, most systems require some combination of these capabilities:

- Seamless signup and login experiences
- Multiple sources of user identities

- Multi-factor authentication (MFA)
- Attack protection
- Granular access controls

Auth0 allows you to quickly address these needs, enabling the team to focus on innovation and advancement of revenue-generating applications and services — rather than continually being drawn into building and maintaining ancillary functions.

But wait ... there's more

While foundational capabilities are important, the real world is ... complicated.

Being able to accommodate change and tailor Identity to your unique needs — and doing both without drawing too heavily upon your development team — is the difference between CIAM as a necessary component of your application stack and CIAM as an operational and competitive advantage.

Satisfying advanced use cases often requires transacting with other business systems and third parties to execute complex conditional flows.

For example, an online retailer might integrate with third parties to:

- Prevent fraudulent registrations
- Protect and enrich existing user accounts
- Stop fraudulent checkouts
- Reward loyal customers

On the other hand, a financial services organization might need third-party integration to:

- Meet regulatory requirements for Identity proofing and consent management
- Help to safeguard wire transfers
- Connect to other financial services providers
- Secure and simplify cash withdrawals from ATMs

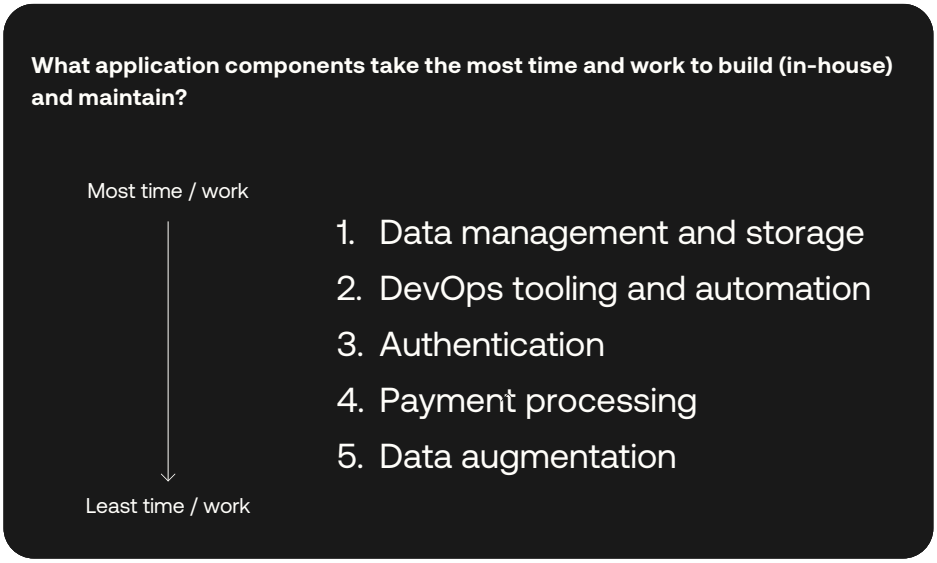
Building such advanced logic from scratch is a major undertaking, and each use case is a custom coding exercise with little that can be reused.

Alternatively, having a simple but effective (read: powerful, flexible, efficient, etc.) way to make Identity work with your other business systems allows developers to quickly implement customized Identity solutions without the time, expense, and headaches associated with custom coding projects.

If preserving developer capacity and speeding time to market matters, buying is the way to go

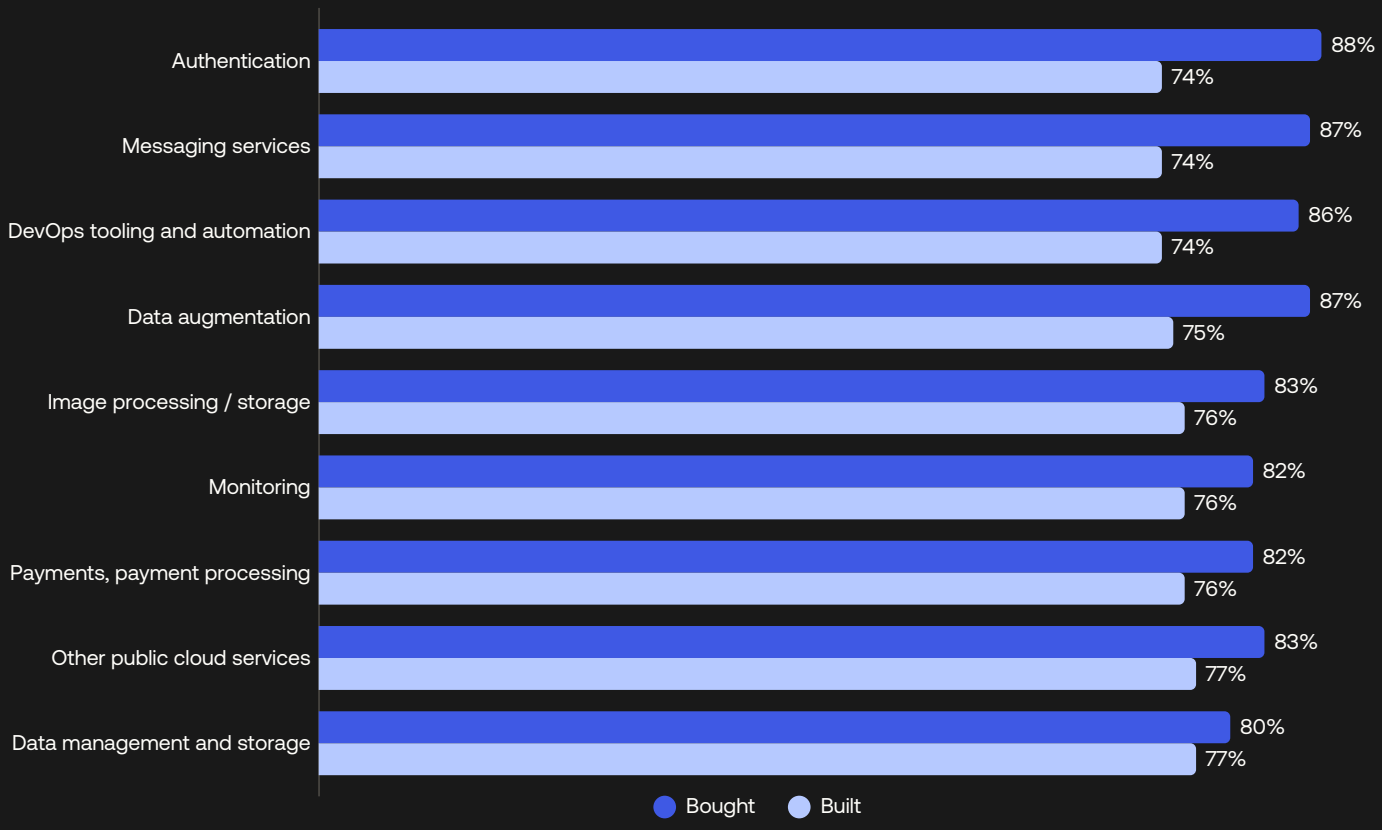
Published in 2023, How development teams purchase SaaS presents the results of a survey of 675 responses from developers, engineers, and IT professionals in 56 countries — and the report shows that purchasing an off-the-shelf Identity solution delivers important business benefits.

For example, respondents reported that authentication functions take the third-most time to build and maintain in house, behind only Data Management and Storage, and DevOps Tooling and Automation.



More importantly, the survey showed that using a third-party authentication solution reduces time to market more than any other SaaS component — **88% of organizations that use a third-party SaaS platform for authentication reported reducing time to market.**

Have you reduced your time to market in the last year?



Impact on time to market from buying third-party SaaS components versus building functionality in-house

Why do organizations large and small choose Auth0?

Here's why organizations from nonprofits and startups to leading global enterprises trust us to deliver convenient, secure, and privacy-conscious experiences for every type of user who needs access to their applications and services.

Unmatched out-of-the-box functionality

With 10+ years as a pioneer in the Identity and Access Management space, we've leveraged cutting-edge technologies and architectures to create a modern solution with an impressive collection of features and functions, including:

- Customizable actions, and pre-built partner integrations
- 60+ social and Identity provider connections
- Broad support for open standards: OIDC, SAML, FIDO, OAuth, and more
- Multi-cloud encryption architecture and support for running on AWS and Azure including public and private cloud options
- Extensive compliance and regulatory requirements from HIPAA to PCI
- Easily customizable and brandable sign-up and login interfaces and flows

As a result, we're with you every step of the way on your Identity journey, from getting started — in just a few minutes with only a few lines of code — to advancing through all four stages of the Customer Identity maturity journey.

Don't make sacrifices when it comes to authentication

	Auth0 by Okta	Other Identity solutions
Out-of-the-box solution	✓	☐
Security center	✓	☐
60+ SDKs and Quickstarts	✓	☐
Integrates in any app written in any language and any framework	✓	☐
Broad support for OIDC, SAML, FIDO, OAuth, and more	✓	☐
Single Sign-On (SSO)	✓	☐
Adaptive MFA	✓	☐
Bot detection and prevention	✓	☐
Breached password protection	✓	☐
Passwordless	✓	☐
60+ social and IdP connections	✓	☐
Compliance and regulatory requirements from HIPAA to PCI	✓	☐
Global developer advocate team	✓	☐
Developer community	✓	☐

A sustainable strategic advantage

Choosing Auth0 means your CIAM needs will be met today, tomorrow, and as far into the future as you can imagine.

We do the hard work of:

- Keeping up with specifications and standards, which makes adding new interoperability and delivering the latest features — like passkeys — as simple as toggling a configuration variable
- Setting the stage for compliance with new and evolving regulations, so you have one less thing to worry about
- Researching threat actor tactics, techniques, and procedures (TTPs) and introducing the advance security features needed to combat these threats
- Exploring how new technologies — including generative artificial intelligence (AI) — can be applied to Customer Identity

All of this means two big things for our customers:

1. Their Customer Identity capabilities are always state-of-the-art
2. They can apply their finite resources on their core value proposition

Extensive developer resources to help your team work efficiently and effectively

Identity is important to your organization, but it's not the reason you exist — and whatever that reason is should be the main focus of your developer and engineering resources.

As much as we care about Identity, we strive to minimize the amount of time you have to spend on it. That's why we offer a pretty astonishing array of developer resources, including:

- **Documentation**: Auth0 Docs, Articles, Quickstarts, APIs, and SDK Libraries
- **Tools**: OIDC Connect Playground, SAML tool, JWT.io, and Webauthn.me
- **Other stuff**: Developer center, code samples, guides, videos, and the Identity Unlocked podcast and Zero Index Newsletter

Everything you need to go after enterprise clients

Your Identity platform should be a valuable tool in your efforts to grow and land larger customers, not a liability that holds you back.

As thousands of organizations have already discovered, Auth0 ticks all the boxes — from the basics like:

- Enterprise single sign-on (SSO), to simplify and secure their login experience
- Robust authorization and access controls that strengthen their security posture
- Multi-factor authentication (MFA) as an added layer of defense against credential theft

To all that extra stuff that can take scaling companies by surprise, including:

- Availability and scalability
- Development, product, and application security
- Compliance and certifications
- Monitoring and logging
- Choice of cloud infrastructure, onboarding and support, and branding

Plus, because every enterprise is different and Identity is an evolving concept, your ability to adapt to change and extend your Identity engine is another important factor.

Once again, we've got you covered with ...

Drag-and-drop extensibility to accommodate and enable your Identity-related use cases

Since launching in late 2020, the Auth0 Marketplace has helped developers quickly find and install third-party Identity solutions for their applications and APIs. Today, the Marketplace includes more than 300 third-party solutions — testament to the "long tail" of Identity functions that are required by today's applications.

Actions Integrations make it even easier to extend Auth0 with partner-built innovations, often with no-code, drag-and-drop ease. Instead of building and maintaining custom code, Actions Integrations are easily integrated third-party solutions that can be quickly added to extend your Identity flow.

In fact, you can even "stack" these integrations like building blocks to keep up with new needs and address advanced use cases.

Security features to protect your organization and customers

As cybercriminals direct more effort and expertise into getting past the login box — including by leveraging the same generative AI capabilities that are transforming society and business — protecting it requires ever-more layers of ever-more sophisticated defenses.

Auth0 has you covered, with:

- Host, platform, and application-layer defenses to filter malicious entities before they can even access the login box or API
- Login-layer defenses that prevent fraudulent signups and account takeovers, including Attack Protection features that can be turned on with a simple toggle
- Post-login defenses to secure sessions and manage access after a user has authenticated
- Observability tools like Security Center that allow you to see potential attack trends and quickly respond to them in real time

Discounted — but still feature-rich — offerings

We're proud to offer a number of discounted offerings that can help you get started and — thanks to a long list of features — are often sufficient for the longer term:

- Self-service options, including a free trial plan that lets you get off the ground with up to 7,500 active users and unlimited logins — while also including social login, DB connection for securely storing Identity information, branded login, extensibility and security capabilities (brute force and suspicious IP throttling), support for five regions (US, UK, EU, JP, AUS), and even passkeys

- Auth0 for startups, which brings the convenience and security of Auth0 to eligible startup customers so they can focus on their core value propositions rather than spending more time than is necessary on Identity
- Our Nonprofit Offering, which provides preferential pricing that makes the leading Identity service even more accessible to organizations on a mission to make the world a better place

Proven results for organizations just like yours

Finally, maybe the best way to learn why other organizations choose Auth0 is to learn more about their own experiences. To do so, please visit our Customers page and check out how some of our startup program members are leveraging Auth0.

Learn more about Identity management with Auth0 by Okta

Disclaimer

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.

Any products, features, or functionality referenced in this material that are not currently generally available may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation, or promise to deliver any product, feature, or functionality, and you should not rely on them to make your purchase decisions.

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871