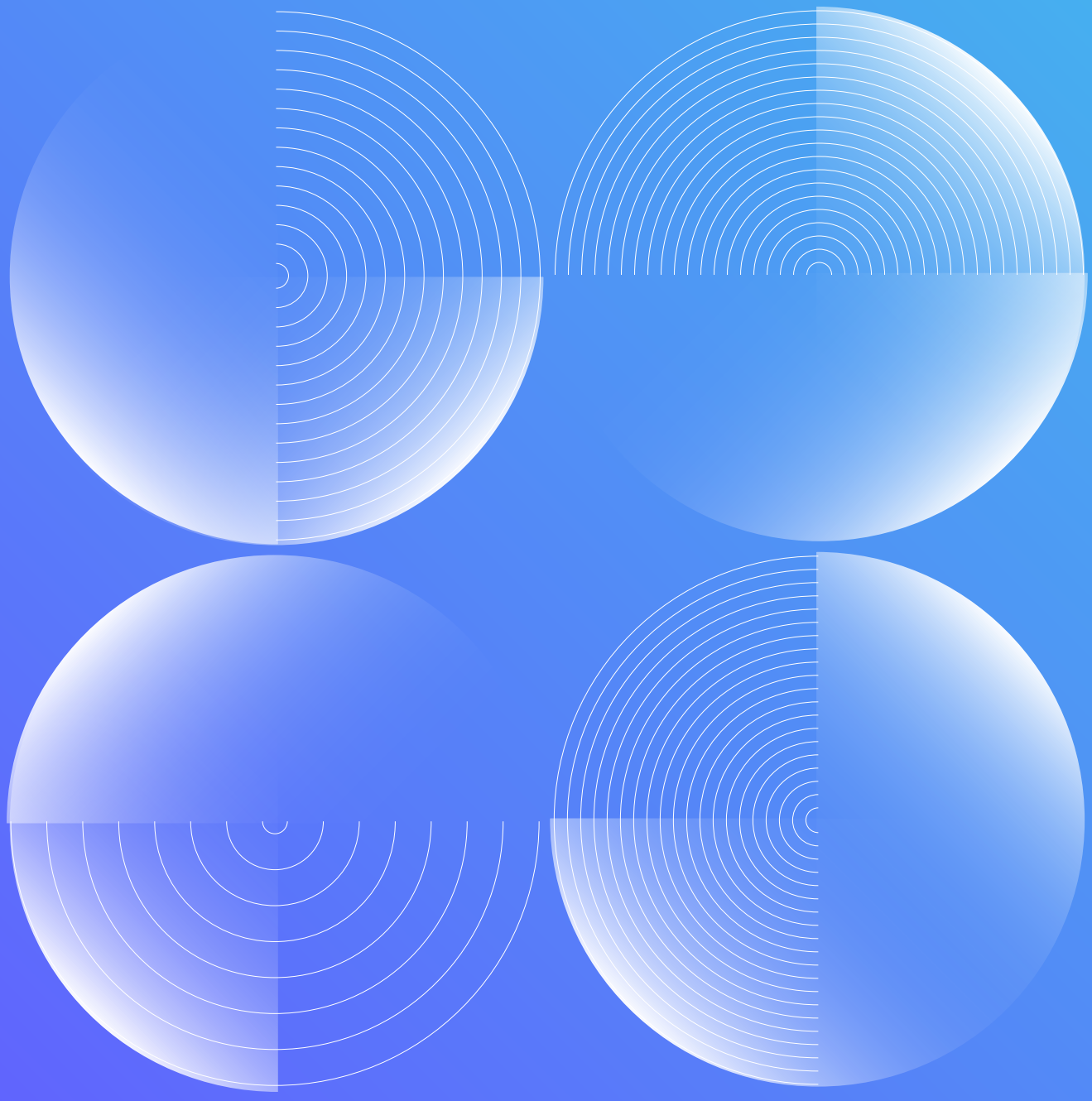
auth0

Enterprise-Ready Identity

A guide to the identity features B2B SaaS companies need to move upmarket and win enterprise customers



EBOOK

auth0.com

Contents

Contents

Introduction

For a small or medium-sized business (SMB), signing a deal with their first enterprise customer is a big deal.

They come with significantly larger deal sizes and higher retention rates, both of which positively influence the lifeblood of any software-as-a-service (SaaS) company: annual recurring revenue (ARR). A recognizable enterprise logo can also decisively impact future sales simply because it is a vote of confidence for future buyers. By landing bigger customers, SMBs send a signal to the market that their product has reached a trusted level of maturity and is now ready for the “big leagues”.

However, there is a cost to doing business with large enterprises. Their needs are complicated, often requiring dedicated investments from both a go-to-market (GTM) and product perspective. SMBs must wrestle with new challenges from onboarding to meeting technical demands. For most businesses, the opportunity for growth presented by an enterprise customer outweighs the complexity. And that’s why becoming “enterprise ready” is one of the most talked-about challenges in B2B technology.

Trading control for opportunity: Meet the new boss

> "The first time you get a few in-bound leads from true large enterprises, you may be confused. You may even be overwhelmed, because they'll quickly identify all your huge feature holes and push you to fill them faster and in a different order and manner than you were expecting."
>
> - JASON LEMKİN, FOUNDER, **SAASTR**

An adjustment for many B2B SaaS vendors is the realization that acquiring enterprise customers often involves surrendering control (e.g., over priorities, the roadmap, etc.) because while SMBs have requests, enterprises have requirements — that's the tweet.

Research indicates that **the average enterprise organization uses 364 SaaS apps**, and the integration and management of that many products isn't possible without imposing strict conditions intended to standardize their introduction and operation. In other words, the enterprise doesn't want to adapt to accommodate hundreds of different apps, it wants each app to accommodate to the way it operates.

And complicating matters, it's a good bet that every enterprise will have a **slightly different** set of parameters. Standards, where applicable, help to multiply the return on effort, but standards compliance often needs to be combined with the flexibility and extensibility to accommodate every enterprise's own unique needs.

For prospective SaaS vendors, all these parameters, policies, and processes quickly impose a long list of requirements. While many of these will have little to do with the core functionality of the SaaS product itself, they are nevertheless prerequisites for all vendors and serve as barriers to filter out companies that are not credible solution providers.

Of course, directing resources to address these requirements can come at the expense of investing in the SaaS product's core functionality — but such is the cost of going upmarket.

Identity is essential to enterprise buyers

Buyers within enterprises are looking for SaaS tools that can enable the organization to sustain and drive growth. However, the sobering truth is that you can have the greatest SaaS application in the world, but if it's regarded as insecure, difficult to integrate, or expensive to administer then it won't clear the hurdles necessary for procurement.

One of the highest hurdles is identity.

Enterprises recognize that if their identity layer (spanning their own workforce solutions and their array of SaaS solutions) works well, then everything from their day-to-day operations to their ability to cope with change and seize new opportunities becomes much easier.

But they also understand that the opposite is true: if there are issues with the identity layer, then even simple tasks become troublesome and time consuming.

Consequently, any B2B SaaS solution targeting enterprise customers must incorporate a comprehensive identity capability — one that likely extends far beyond the basic **authentication, authorization**, and identity management functionality that satisfied SMB customers.

Whether your plan is to try to build such functionality in house or to source a third-party solution, understanding what enterprise customers will require is a necessity.

In this guide, we will walk through both the identity requirements and the ancillary functionality that enterprises need, while also highlighting what you — the B2B SaaS vendor — need from your customer identity implementation to sustainably scale your business.

Enterprise Identity Requirements

To ensure their SaaS apps efficiently and securely enable the organization, enterprises have a handful of identity requirements. These are the features that B2B SaaS products must meet in order to be considered as enterprise-ready by evaluators.

Enterprise single sign-on (SSO)

> **"Once we built Kandji's core product, we thought about how we could appeal to larger businesses. It really does start with authentication as that's the first touchpoint a user has with an application. As we grew, we realized that we had to include an SSO solution that could cover a good amount of the market."**
>
> - TİM GUMTO, SENİOR TECHNİCAL PRODUCT MANAGER, KANDJİ

With federation, your product outsources authentication to the enterprise's owned-and-operated identity provider, which is responsible for authenticating the user, applying access policies and, upon successful authentication, sending the user into your product.

Leveraging federation, SSO allows multiple applications to use the same authentication session, thereby avoiding repetitive credential entry and the fatigue that it causes. This is particularly important to enterprises because they typically will have many different services and a large number of end users. Additionally, SSO is usually a component of an enterprise's security strategy—with fewer credentials to remember, fewer credentials can be forgotten by enterprise users or stolen by bad actors.

But the benefits go beyond security: SSO also improves the experience for the enterprise's users and can help to reduce IT administration and support costs. Administrators can easily manage user provisioning and de-provisioning via their own identity provider, and users are less likely to need to contact support because of forgotten credentials.

Finally, because it enables scale, self-service configuration is key to successful federation. Many identity implementations stop short of providing this, which results in significant manual work on the part of customer-facing operations, sales, and support teams. By allowing your customers to configure SSO on their own, you can accelerate the proof-of-concept process, troubleshooting, and customer onboarding after a sale.

Standards can be a dealmaker

There are a number of standards that make federation and SSO possible, **including SAML, OAuth, and OpenID Connect-based systems**, which enable federation through leading Workforce Identity providers like Okta, Azure AD, and Google Workspace.

Supporting these standards is the key that unlocks federation and SSO; consequently, as new options emerge the pressure will be on you to support them. If you're building an in-house solution, don't overlook the need to continually maintain and extend your functionality to accommodate evolving identity requirements.

Authorization and access control

> "Proper authentication is so important for our customers to keep sensitive organizational data, like real time dashboards, secure."
>
> - BRİAN DEWANGGA, PRODUCT MANAGER, **SCREENCLOUD**

To control which users can see what data and perform what actions, enterprises require a way to grant and manage appropriate levels of user permissions throughout an application.

Historically, software applications handled authorization in a fairly coarse-grained manner in which a user has one or more roles in an application, granting them permissions to perform certain actions within it. This approach was sufficient so long as users didn't create content in systems. But, as social and work collaboration applications were adopted, a different kind of authorization became necessary.

Over time, and partly driven by the goal of implementing the security **principle of least privilege access**, several different approaches emerged, with each providing more flexible access control:

- Attribute Based Access Control (ABAC)
- Role Based Access Control (RBAC)
- Relationship Based Access Control (ReBAC)

Today, RBAC is the minimum level of control that most enterprises will require because it enables application administrators to manage the permissions of users within a team.

As we will examine shortly, security, compliance, and privacy measures are musts to be seriously considered by an enterprise, and strong and flexible authorization helps to address these requirements.

However, solving authorization in an application is not trivial, and enterprises will look for applications with authorization that is:

- **Reviewable:** It should be easy to determine "who can access what," to understand the rules used to enforce access control.
- **Easy to manage/change:** Authorization-related changes must be explicit and traceable. Change management control for authorization is important.
- **Auditable:** It should be possible to know what happened with regard to authorization, in essence "who tried to access what, and when?"
- **Fast:** Authorization decisions are made as part of most flows/requests, so they can't introduce latency.
- **Reliable:** Authorization components need to always be running and returning the expected results.

Get ahead of the curve with fine-grained authorization

As privacy and security awareness increases in the industry, the need to apply the principle of least privilege across organizations is becoming more of a product requirement than a 'nice-to-have' feature. One result of this shift is that enterprises are recognizing the benefits of fine-grained authorization (FGA), which goes beyond traditional Role Based Access Control (RBAC) to enable greater flexibility for enterprises with complex permission models.

FGA allows organizations to centralize access control across every application they build or acquire, and makes it easy for application developers to implement advanced permissions and sharing strategies. This is 'fine grained' because there is no limit to the granularity at which builders of the system can make authorization decisions — application builders have the freedom to determine precisely how granular they want authorization to be, and users are granted control to determine who has specific permissions on objects they manage.

Collaboration and social features (e.g., the "Share" button) are things modern software users expect, even in enterprise contexts, when collaborating on documents, spreadsheets, design mockups, project boards, etc., and FGA allows the easy sharing of these objects between users in a scalable manner.

Learn more about fine-grained authorization

Multi-factor Authentication (MFA)

> "Security is a key consideration for enterprise customers, and we would not have been able to close many deals without having MFA and SSO available."
>
> - QASEEM SHAİKH, CTO, **SENDOSO**

Multi-factor Authentication (MFA) aligns with enterprise security policies by validating that the owner of an account (or set of credentials) is actually the one trying to access the application. It does so by requiring users to provide two or more authentication factors before being granted access to the requested resource — in this case, your SaaS application.

MFA could arguably fit into the security section below, but in recent years **attacks against identity systems have become so common** that MFA is fast becoming a standard enterprise identity requirement.

For context, consider that **Verizon's Data Breach Investigation Report (DBIR) 2022** revealed that:

- Almost half of data breaches start with stolen credentials, making account takeover the number one threat for employees and customers.
- Over 80% of the breaches involving attacks against Web Applications can be attributed to stolen credentials.
- The top two data types exfiltrated by attackers are personal data and credentials.

Faced with this reality, it's only natural that enterprises want to ensure there are additional defensive layers protecting access to their SaaS systems. Implemented correctly, multi-factor authentication is one of the most effective layers.

Having to overcome MFA drastically increases the time and effort needed for the attacker to compromise the account, which makes it infeasible to do at scale. However, it's essential that the solution is implemented properly (i.e., without errors and omissions that leave vulnerabilities) and uses strong secondary authentication factors. Plus, you must also consider usability, although the preferred balance between security and usability will vary from enterprise to enterprise (which is another reason why it pays to be flexible).

One way to assess the quality of user experience is by examining two measurements:

- The passing rate of an authentication challenge: the higher the passing rates, the better the user experience.
- The time to complete an authentication challenge: the shorter the time to complete, the better the user experience.

Combining these two measures and comparing across different authentication challenges shows that the user experience varies significantly. Visually examining Figure 1 reveals that:

- Voice and email authentication provide a poor user experience: passing rates are comparatively low and the time to pass is comparatively high.
- Push via a proprietary application, pushing a one-time password (TOTP), and using SMS as an MFA channel deliver a middle-of-the-pack experience.
- Leveraging **passwordless challenges** like device biometrics (WebAuthn) delivers the best user experience, as indicated by high passing rates combined with a low time to complete the challenge.

We can also see a high degree of correlation between those authentication challenges that deliver a convenient user experience and those that provide the best security.

In fact, WebAuthn-enabled biometrics are a powerful example of how CIAM systems can simultaneously deliver a convenient, private, and secure experience.

Figure 1: Internal Auth0 data shows that WebAuthn-enabled MFA minimizes friction and enhances security

Stand out from the crowd with biometrics

Authentication methods based on WebAuthn-enabled device biometrics (e.g., Apple Face ID, Apple Touch ID, Windows Hello) or security keys (e.g., YubiKey, Feitian, Titan) offer an unmatched combination of strength and low user friction and represent a big step forward for security and user experience.

Implemented via a WC3 Web API, WebAuthn allows browsers to authenticate using a public/private key pair generated for each user/device/website, instead of shared secrets. Importantly, because it guarantees that credentials are only valid for the websites where users actually registered, the method is not vulnerable to phishing.

WebAuthn is relatively new, so adoption remains fairly limited at this time; nevertheless, WebAuthn holds tremendous appeal for both users and application providers, so enrollment is expected to grow substantially. While WebAuthn may not yet be a strict requirement for enterprises, it may soon become so — and supporting it today will help you to stand out from the crowd.

Learn more about using WebAuthn-enabled biometrics and security keys to enhance security

Beyond the basics

The features described above are likely to be required by enterprises, but that doesn't mean they are enough to satisfy the requirements of all enterprises.

For example, some enterprises may require **identity proofing** as an added layer of protection for access to critical services.

Others may favor usability for some SaaS applications, leading them to require the advanced functionality of **adaptive MFA** and **step-up authentication**.

Adaptive MFA is a technique that only engages MFA when a user interaction is deemed risky based on behavioral data (e.g., an unknown device, impossible travel, IP reputation, risk scoring, etc.).

By reserving MFA for risky scenarios, adaptive MFA maintains security while preserving the frictionless experience for the majority of users.

Step-up authentication also empowers application providers to strike a balance between security and friction, in this case by adapting identity requests to the importance of the resource and the risk level if it were to be exposed. It ensures users (or whomever might be posing as a user) can access some resources with one set of credentials but will prompt them for more credentials (e.g., MFA) when they request access to sensitive resources.

Leverage extensibility to reduce perceived risk

These are just a few examples of additional identity features that your enterprise prospects and customers may require — the list of potential features is long and always growing.

Even if an enterprise doesn't require a particular feature (or standard) today, they may require it tomorrow — and they will expect all of their SaaS vendors to be able to rapidly support this need.

Demonstrating an ability to extend today's functionality to accommodate tomorrow's requirements can go a long way to reducing the risk associated with choosing your solution by future-proofing that decision.

And being able to do so without draining resources better applied elsewhere is essential for your own company's sustainability.

Learn more about the power of extensibility

Additional Requirements

It isn't enough to deliver the identity features the enterprise needs — those features have to be delivered in a way that satisfies a collection of additional requirements.

In fact, it's this set of requirements that often separates a solution that meets the needs of SMBs from one that is truly enterprise ready.

Availability

The enterprise is considering purchasing your SaaS application because they need it to fulfill one or more functions, and they want to be certain that it will be able to fulfill those functions all the time. Anything less is unacceptable.

There's an adage in professional sports that "the best ability is availability" and this sentiment extends to the enterprise world.

You can expect enterprise prospects to ask about the availability of your SaaS solution — including the number of nines in your uptime, failover models, **service level agreements (SLAs)**, and disaster recovery — but the same line of inquiry extends to critical components like identity. Whether you build your solution in house, incorporate third-party elements, or essentially offload to a CIAM provider, you will need to be able to demonstrate that the identity engine will be available at all times.

Scalability

Even SaaS providers who recognize that enterprises have unique needs can fail to appreciate some of the nuances.

First, enterprises can be big. Really big. Perhaps the most basic requirement is to scale to support thousands, and even many tens of thousands, of users. Maybe these users are spread around the globe, maybe they're concentrated in one region, or maybe they fall somewhere in between. The distribution has implications for where and how you host your services, and where and how offloaded services (e.g., identity) are hosted.

Second, enterprise needs can change suddenly and significantly. An enterprise might initially roll out your SaaS application to 10% of the workforce but then — without warning — decide that it's worth extending to 50%.

And third, as noted above, identity decisions themselves need to be fast. A login screen stuck on a “waiting…” message or that experiences timeouts is a very visible deficiency, so keeping up with identity transactions and executing them with minimal latency is essential.

Scale can bring with it a lot of problems, and unfortunately these often don’t become apparent until you run into them: there’s a massive difference between a minimal viable identity functionality that works during a demonstration, or even for SMBs, and one that is truly enterprise ready.

Multi-tenancy matters

Marc Benioff, co-founder of Salesforce and noted technology luminary, famously stated that, “Multi-tenancy is a requirement for a SaaS vendor to be successful.”

While single tenancy may not have prevented you from winning and delivering for SMBs, as you begin to scale and grow you will come to appreciate the truth of Benioff’s words.

It really is worth repeating: multi-tenancy is a requirement as you aspire to win enterprise business. That’s because only an effective multi-tenant environment can overcome the complexities associated with serving enterprises, like meeting their availability and resource demands while making efficient use of infrastructure (to manage your costs) and preserving data security.

Ultimately, multi-tenancy reduces the cost, overhead, and chaos of running a SaaS solution because it promotes efficiency through shared resources. On the back end, it simplifies engineering efforts and reduces the technical debt that provides friction against growth. These benefits apply whether the context is your application as a whole, or your identity infrastructure.

Identity security

In a world of ransomware, data breaches, and credential theft, security is considered table stakes (translation: an absolute requirement) for enterprises. At some point in the procurement process, an IT manager or security leader is going to ask tough questions about:

- Development security
- Product or application security
- Operational security

EnterpriseReady offers a fairly comprehensive overview of all three, and depending upon your identity implementation, each of these areas may apply to your identity infrastructure. We don't want to repeat what's already included in that great resource, so instead we'll briefly examine operational and product security.

First, to meet the enterprise's availability requirements, you need to ensure that your identity infrastructure can withstand the more generic (i.e., not attacking identity itself) threats including denial of service attacks. If you're looking at an identity vendor, be sure you understand how they defend against such attacks, because you'll likely need to provide those answers to prospective enterprise customers.

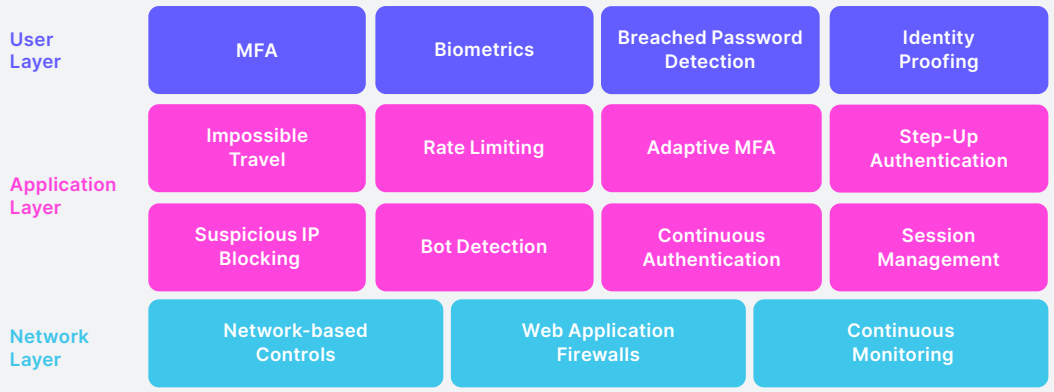
Second, when something goes wrong with identity, the impacts can be far-reaching, which means securing identity is critical to helping the enterprise to maintain a strong cybersecurity posture.

As attackers focus greater attention on attacking identity systems and evolve their tactics, techniques, and procedures (TTPs), it is essential that:

- Your identity solution includes defense-in-depth tools that work in combination across the user, application, and network layers (Figure 2)

- You (or your identity provider) continually monitor your identity component for signs of attacks and changes in TTPs
- You (or your identity provider) make adjustments as needed, like turning parameters, tightening restrictions, introducing new tools, etc.

Figure 2: Securing CIAM requires a defense-in-depth strategy employing many complementary tools and techniques



Identity is under attack

As we explore in our annual **State of Secure Identity Report**, your login box is under attack from an assortment of threats, including:

- Fraudulent registrations
- Credential stuffing
- MFA bypass
- Password spraying and password guessing

And that's not all: session hijacking, session ID URL rewriting, and injection also present threats, and breached credentials and

automation tools have lowered the barriers to entry for prospective attackers.

These attacks can lead to a range of consequences, including service degradations (or even taking your identity component completely offline) and account takeovers (ATOs) that compromise sensitive data and can be used as initial access vectors.

Enterprise buyers are educating themselves on these threats, so it's imperative **you have good answers ready** when they start asking questions.

Compliance and certifications

There is little chance that an enterprise buyer will risk their reputation (and career trajectory) on a home-built solution unless you can show the requisite array of logos to satisfy their requirements.

Certifications such as SOC2, ISO27001, and PCI DSS demonstrate to enterprises that you are serious about managing customer data, information security, and payment data, respectively, although they represent only the tip of the iceberg.

Enterprises with international operations must comply with a complicated set of data processing, storage, and privacy laws, and regulations, such as General Data Protection Regulation (GDPR), General Personal Data Protection Law (LGPD), Act on the Protection of Personal Information (APPI), Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA) impose different requirements depending upon where enterprises operate.

In addition, standards and regulations are constantly evolving, so maintaining certifications and compliance is an ongoing obligation.

Compliance earns conversations, but certifications win deals

Loosely speaking, “compliance” is a claim that a system fulfills certain regulatory obligations and requirements (e.g., adhering to a standard), while a “certification” means that an independent third party has validated those claims.

To enterprise buyers, evaluators, and influencers, **certifications are worth much more** than mere claims.

Monitoring and logging

For a number of reasons — ranging from business analytics through compliance, audits, and full-scale incident response — enterprises need detailed visibility into their applications.

In short, they need to be able to understand:

- **The past:** Who has access to what resources.
- **The present:** Who accessed what resources and performed what actions.

At a minimum, meeting this requirement means having detailed audit and system logs that enterprise administrators can import into their existing systems, although other teams may prefer a built-in reporting interface.

Additionally, you can safely assume each team will have a different reason for needing visibility, so the more detailed and granular your logs, the more likely you will be able to satisfy an enterprise’s requirements.

Don’t overlook your own visibility needs

Monitoring and **logging** aren’t just important for your customers, but also for you, to enhance your understanding of how customers are using your SaaS application.

This information can help you spot upsell opportunities, recognize and adjust to threats, anticipate emerging needs, and extract insights about your customer base (made practical by a multi-tenant architecture).

Other potential requirements

Here are a few other potential requirements you may encounter as you go upmarket:

- **Choice of cloud infrastructure:** Some enterprises — particularly those with more complex development processes, region-specific regulatory hurdles, and high-performance needs — may have strategic, geographic, or technical requirements about what cloud providers your SaaS product may use. It is therefore important for your product and its components to provide different public and private cloud options.
- **Onboarding and support:** After an enterprise buyer chooses a SaaS solution, they expect that solution to be introduced and adopted quickly. Demonstrating a mature onboarding process and supporting resources (e.g., self-service options, APIs, documentation, tutorials, etc.) create confidence that your product will not slow things down.
- **Branding:** Allowing customers to customize their experience with their own branding may seem like a “nice-to-have” feature, but for many enterprises, it truly is a requirement.

Summing it all up

“Our core competency is building tools for organizational transparency, it’s not authentication.”

- TYLER DAVIS, CEO AND CO-FOUNDER, **LAUNCHNOTES**

Going upmarket is frequently a goal and sometimes a necessity 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 like 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.

At a minimum, they will likely demand:

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

Beyond providing these identity features, your identity component must also satisfy expectations around:

- 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 an important factor.

It's not impossible to code these capabilities in-house, but doing so is very challenging and requires specialized subject matter expertise.

For most B2B SaaS vendors who aspire to break into the enterprise market, the fastest, most efficient, and most cost-effective way to satisfy these new requirements is to integrate a proven CIAM solution from a best-of-breed vendor.

Doing so turns identity from a potential weakness into a strength — from just another thing you have to do into an opportunity to stand apart from competitors — and can convert influencers within IT or security teams into champions who advocate on your behalf.

And, leveraging a trusted third-party CIAM provider allows you to focus on what you do best, as you look to win more enterprise customers and continue to grow.

Grow your SaaS applications, one login at a time

Your identity platform should be a valuable tool in your efforts to grow and land larger customers. Auth0's Business Customer Identity solution is **purpose-built for the unique needs of B2B SaaS organizations**. With it, customer requirements around enterprise SSO and MFA are available out-of-the-box. Coupled with our high availability cloud services that ensure a 99.99% SLA, you'll have another great reason for that larger customer to sign on the dotted line.

Development teams can quickly implement Auth0 into your application with well-documented APIs and SDKs. In fact, many of our customers go live in less than a month and have been able to shorten their time to market for other key product capabilities.

You'll also have the peace of mind of having an on-demand, identity security system in place. Secure the data of your business customers by quickly adding protection against some of the most common attacks on identity systems out of the box. From bot attacks to credential stuffing, Auth0 takes the burden of identity security off your internal teams so that they can focus on shipping new features for your product.

Importantly, all of this can be managed programmatically and at scale using **Auth0 Organizations**, which can help you represent all your business customers in your multi-tenant application.

→ Learn how LaunchNotes up-leveled identity and won enterprise business within a week

→ Learn how modern identity helps Sendoso win enterprise business

→ Learn how Kandji implemented enterprise-ready identity despite limited engineering resources

Auth0 is an easy-to-implement, adaptable and secure authentication and authorization platform. Built on a set of composable building blocks exposed through APIs and protocols, the Auth0 Identity Platform provides multiple solutions to address any identity use case without forcing a compromise between convenience, privacy or security.

Learn more at **auth0.com/identity-platform**