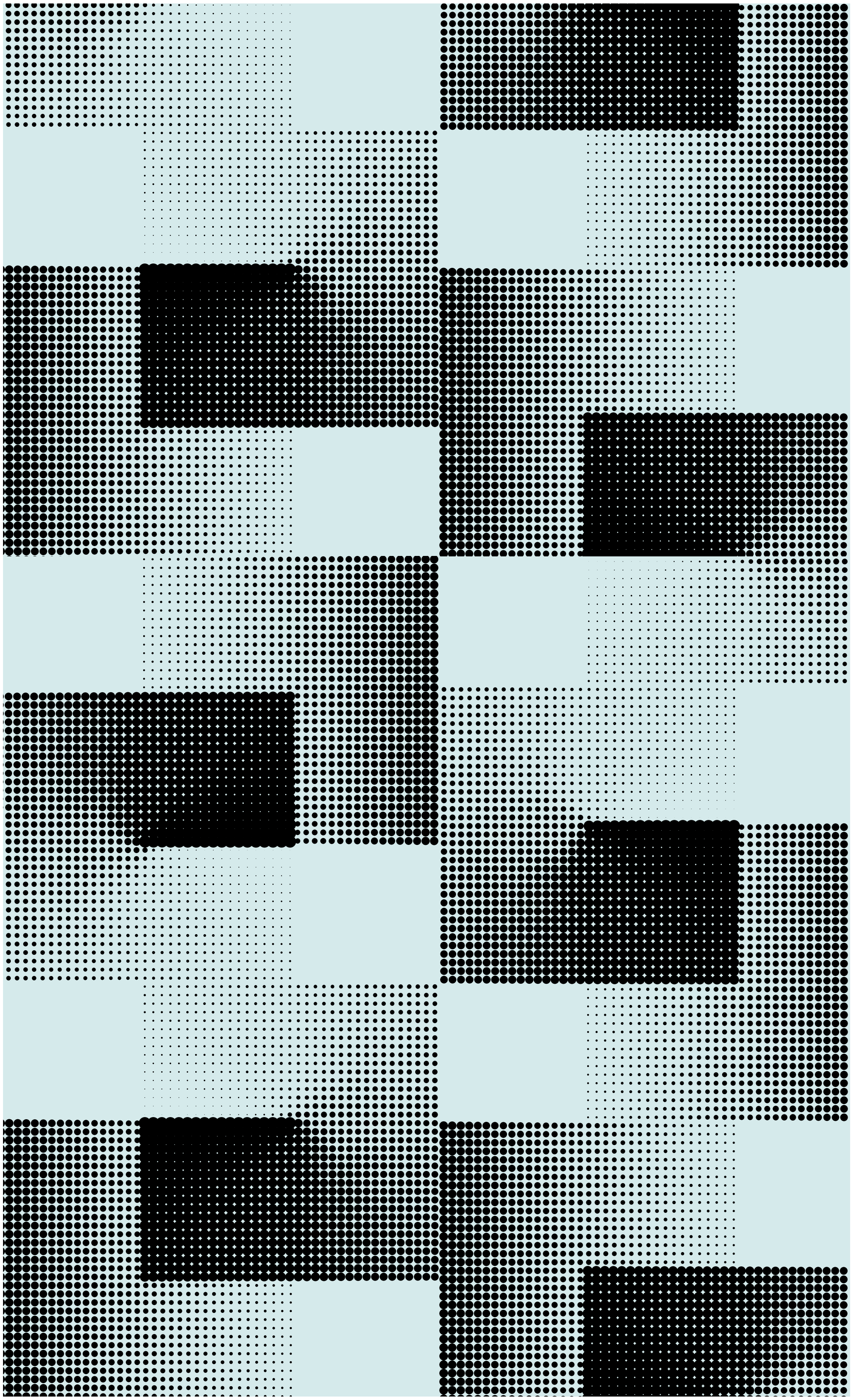
Whitepaper

November 2020

Build vs. Buy

Roll your own auth vs. embed a pre-built identity layer into your app

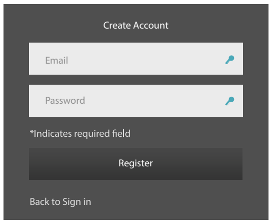
Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



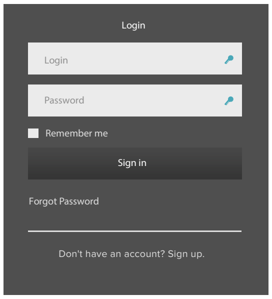
Contents

Every team building a new web or mobile application faces a choice: build the entire application in-house or selectively use out-of-the-box services to make the job easier and faster. Many of today's successful teams have chosen the latter with services like Stripe and Braintree to offload payments and Twilio to offload communications. A third-party customer identity and access management (CIAM) solution is another such service. A digital identity layer comprised of APIs, SDKs, and out-of-the-box customizable components can serve as building blocks to increase speed-to-market, lower development costs, and focus in-house developers on the core features of the application.

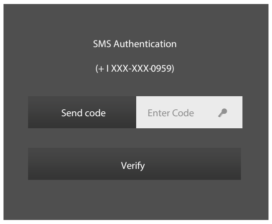
Customer-facing applications—whether they are aimed at consumers or business users—require a common set of fundamental features related to authentication, authorization, and user management. Applications need to support common workflows such as account creation, user login, password reset, account recovery, and multi-factor authentication (MFA) enrollment. Additionally, applications need to accommodate different levels of access depending upon the user.



*Indicates required field



Don't have an account? Sign up.



Architects and engineering leaders are often unsure about whether a comprehensive identity and access management (IAM) solution from an outside vendor is right for their project. This whitepaper discusses the key considerations when making a build vs. buy decision and the advantages of a pre-built solution.

The Challenges of Identity and Access Management

Identity and access management for customer-facing applications includes functions like authentication, authorization, and user management. Authentication allows a user access to a system via password, token or API key, outside directory such as Active Directory or LDAP, enterprise IDP, or social login. Authorization defines what resources they can access. User management includes the storage and security of users' personally identifiable information (PII), managing the lifecycle of the user from sign-up to deletion, as well as more advanced features like single sign-on and provisioning to downstream applications. End users take much of this core functionality for granted, but executing on the project plan entails a variety of challenges:

Complexity

In-house development resources may be able to handle identity basics such as account creation, login, and password reset. However, customers today are increasingly demanding greater functionality and security, which oftentimes increases the scope of projects. Advanced features like single sign-on support, customer data partitioning, token authentication, multi-factor authentication, social login, and LDAP/Active Directory integration, require considerably greater effort to build. Additionally, companies quickly begin to build additional applications and may find themselves reinventing the wheel if development teams are not in constant communication. As a result, individual teams often underestimate the difficulty of building a complete, future-proofed identity service, which causes deadlines to slip. And, identity requirement are constantly evolving. SAML and WS-Fed have evolved to more modern standards like OpenID Connect and OAuth 2.0. Elements within these standards have evolved as vulnerabilities have been found. Further, enterprise requirements such as deprovisioning access to APIs by revoking tokens may not have been initially contemplated in the standard.

Common Identity and Access Management Requirements

Component	Description
Terminate SSL	Create and maintain a secure connection with any client over https. Manage a web certificate for a domain. Setup and maintain/patch strong SSL/TLS. Keep cryptography up-to-date.
Operating system set-up, maintenance and lockdown	Customization of operating system and server software to eliminate security vulnerabilities.
Password storage and security	Hashing of passwords with most up-to-date algorithms and continuous maintenance as methods evolve.
Reporting	Dashboard of metrics to see overall health of users and applications. Easy access to user reports for compliance purposes.
Deploy token service	A scalable service to track each user session, with ongoing database maintenance and patching.
Deploy directory with extensible profile/user/ groups/clients	A scalable user repository that provides a flexible user profile and groups. Includes Directory App server, Database, App Database, and Encryption.
Admin UI	Admin user interface for managing users, apps and APIs with scoped admin roles.
Customer UI	Customer service or help desk UI to manage customer profile information with scoped admin roles.
Registration, sign-in, account recovery, MFA screens	Building user interfaces and workflows, hosting of sign-in and registration pages.
Implement protocols	Learn and amortize specs for SAML, OIDC, OAuth 2.0.
Build authorization server	Build authorization engine for business logic, including customizable scopes and claims.
Social auth and profile sync	Broker authentication for any social identity provider, and sync profile attributes.
SSO connectors	Custom-build, maintain and test SSO connectors for third-party apps.
MFA	High availability, redundant MFA with multiple factor support (SMS, voice, email, Google Authenticator, biometrics, Push).
Authentication policies	Configurable policies and policy framework to control sign-in based on context such as user, app, group, geolocation, IP range, behavior, device, etc.
Provisioning engine	Engine for managing user objects in downstream services.
Provisioning connectors	Custom-build, maintain and test API-based connectors to hand CRUD functions.
Directory/IDP integration	Create integrations with outside directories such as AD/LDAP and support inbound federation via SAML, OIDC and WS-Fed for existing IDPs.
Gateway integration	Integrate with API gateways such as Apigee and Mulesoft.

Alignment of Resources

Organizations frequently lack the very specialized resources required to build a secure and scalable identity function for their applications. It requires team members with diverse technical knowledge, including cryptography, database security, performance engineering, system engineering, and security auditing, as well as advanced data architecture to manage authorization. This is one reason that large companies like LinkedIn and Salesforce have identity teams of twenty-five or more—just to maintain user management. Specialist development resources are scarce, which means many organizations will have trouble finding the resources to get the job done in-house.

Availability

Customer-facing applications require extremely high availability to ensure that end users are able to log in regardless of the load on the application. In the event of a problem with the user management backend, the app breaks and the customer experience is ruined. This undermines the ability of the application to do the job it is designed to do—enhance the customer experience and drive revenue. One bad online experience can damage customer trust, nudging them in the direction of a competitor.

Common Requirements for High Availability

Component	Description
DDOS protection	Automated rate limiting across all endpoints to thwart DDOS attacks. Frequently requires work additional to IaaS capabilities.
DevOps	Systems and on-call operations team to deploy and manage the service in real-time. Automated machine config, database backups with aging and fidelity testing, and privileged access management.
Infrastructure availability	Implement automated monitoring and management of machine resources (removing down nodes, deploying replacements).

Scalability

Companies find it hard to predict user volumes for their applications, and as a result can become victims of their own success. If too many users try and log in at the same time—for example in response to a major news event or feature release—your identity service must be able to handle the workload. Resource-intensive actions like authentication, password encryption, and search need to scale with user demand during these peak periods. Companies need to consider loads across their various production, QA, development, continuous integration and disaster recovery environments and buffer for overprovisioning. High volume applications can require dozens of servers to handle user management. And the risks of scalability are high—online customers will simply leave if they can't log in to the application.

Security

User data breaches are very public and very expensive. Applications are a gold mine of personally identifiable information (PII), often including sensitive data like social security numbers, credit card numbers, and more. The security environment changes constantly, and data hacking techniques have become super-charged with the power of cloud computing. **Recent research** has shown that the average application has a staggering 26.7 serious vulnerabilities, the majority of which comes from custom code. Registration, login, and recovery workflows are frequently the most exploitable attack vector, resulting in application security risks such as broken authentication, broken access controls, sensitive data exposure, and insufficient logging and monitoring listed amongst the **OWASP Top 10** every year.

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

Common Requirements for Maintaining Security

Component	Description
Security monitoring within engineering	Automated logging and monitoring of all activity within the service including admin actions, app behavior, file integrity, change control, intrusion detection. Controls on-data transport attempts. Alerts for suspicious behavior to on-call DevOps and Security teams.
Security monitoring tools	SIEM for security monitoring (Splunk, AppD, New Relic, Zabbix, Wavefront, etc.).
Secure engineering practices	Organizational controls and third-party auditing of software development. • Security code reviews • Vulnerability scanning on codebase • End-point security and authorization controls • Third-party penetration testing • Bug bounty program
Regulatory compliance	Processes to obtain and maintain certifications, accreditations and compliance for: SOC 2 Type 2 Certification, ISO 27001, CSA Star, TrustE, FedRamp, GDPR, Open Banking, PSD2, SMART on FHIR.
Reporting UI	Security and compliance UI to manage event information with scoped admin roles.

The Challenges of Identity and Access Management

Engineering leaders have grown more aware of the difficulty of building, securing, and maintaining user infrastructure, and they have proactively sought out solutions. Rather than sacrifice features in the face of rising complexity, they increasingly offload the identity layer of their apps to third-party customer identity and access management providers. This approach has a variety of advantages over building it in-house. Specifically:

Accelerate Time-to-Market

Development teams experience a lot of pressure to deliver web and mobile applications on time, and because the market is increasingly competitive, timelines are more ambitious than ever. Any delay in time-to-market threatens to reduce revenue, and risks losing a prospective customer. Offloading identity to a trusted third party helps ensure your team delivers on time.

Example cost of delayed time-to-market per project or initiative:

$50K × 6 = $30K

expected monthly revenue — month delay — lost potential revenue

*As the number of projects and initiatives increases, each with its own custom-built auth, there can be massive replication of efforts.

> “
>
> [Okta] is one of the things that I can put in my toolkit to say: Hey, we’re gonna move faster because we have this identity component nailed.
>
> Scott Howitt,
> CISO, MGM Resorts International

Lower the TCO of Application Development

Identity management is one of the highest-risk areas for cost overruns, because feature and system complexity are so often underestimated and in a state of constant evolution. A home-grown approach introduces greater uncertainty into the equation and costs increase significantly when internal teams get sidetracked on building deep user features or discover that their requirements have transformed due to a changing landscape. Teams may still deliver on time, but only with the help of costly contract resources.

When you offload identity to a trusted provider, you help ensure the development team delivers the full scope of your project on budget.

Example TCO reduction of application development:

3	×	6	×	$200K	×	90%	=	$270K
developers		month identity timeline		fully loaded salary		improvement		reduction in TCO

> Things in the identity space change almost by the hour, and we need a technology partner that can keep up with that pace of change on a daily basis.
>
> Eash Sundaram
> EVP Innovation, Chief Digital & Technology Officer, JetBlue Airways

Focus Resources on Core Application Functionality

Your success depends upon how well you execute the core product features that make your application useful to end users. A modern identity layer frees your team to remain laser-focused on functionality that drives revenue and customer engagement; and allows your developers to more quickly move onto the second, third or fourth app that your customers are demanding.

Example opportunity cost of diverted resources:

$$\frac{\overset{\text{annual EBITDA}}{\$10M}}{\underset{\text{developers in org}}{50}} \times \underset{\text{developers on project}}{3} \times \underset{\text{month identity timeline}}{6} = \underset{\text{lost earnings opportunity}}{\$300K}$$

*Common Google-esque calculation of the value of an engineer for companies where the technology is the primary generator of revenue. Here, we are calculating the average annual revenue contribution of an engineer multiplied by the number of engineers that are removed from the engineering pool to deliver an identity layer.

> “I don’t want to reinvent the wheel in our identity stack. I want to use what’s best in class in the market and then apply the Adobe-specific requirements to that stack to get something out to our customers really quickly. Using Okta at Adobe has allowed my organization to focus on the key differentiators in our product, building value for our customers and investing our time and efforts in the things that make our customers successful.
>
> Scott Castle
> Director Product Management, Digital Media, Adobe

Reduce the Risk of a Security and Compliance Breach

When was the last time your team updated their password hashing algorithm? User data and PII are the most common target of attacks. The average lifespan of an effective encryption algorithm is 18 months, but protecting users often falls by the wayside in favor of requirements that drive growth or revenue. A secure identity service requires your team to have knowledge—and time—to address vulnerabilities at every layer of infrastructure, from the operating system, database, and transport layer to the application stack and code vulnerabilities. Because development teams rarely have this level of security expertise on staff, they don’t know their user security has failed until sensitive data is already compromised. And they often aren’t aware of security developments, like when an algorithm has been compromised, or an attack vector is discovered. A well-chosen identity management service safeguards your user data from attackers, because the team that built it is comprised of experts entirely focused on advanced security to cover identity and access attack vectors. Security measures include powerful encryption, API security, advanced firewall protection, and robust data management and system access procedures. These same security measures and infrastructure enable your teams to be compliant with geographic and vertical-specific regulations such as HIPAA, FedRamp and GDPR.

> “
>
> Okta helps us be HIPAA-compliant… largely because we don’t have to go in and manage and maintain the identity of our customers, we trust Okta to do it.
>
> Rish Tandon
> CTO, Heal

Help Ensure a Better User Experience

Functions like account creation, login, password enforcement and session management determine the user’s first impression of your application and by extension, your company. When these elements of the digital interaction are less than perfect or less than seamless, users lose trust and will take their business to your competition. A pre-built identity service focused on frictionless customer experiences across a wide variety of use cases offer a head start in building that user experience. From out-of-the-box, customizable and hosted self-registration/login screens, to passwordless experiences, to single sign-on and social login— the leading customer identity providers offer user experience features that can be implemented with little to no custom code.

> “
>
> National Bank of Canada services millions of clients in hundreds of branches across Canada. As an organization, we have clear objectives, one of which is to simplify the customer experience. Okta’s smart authentication and contextual capabilities enable us to give our clients a seamless, secure online experience.
>
> Rish Tandon
> CTO, Heal

Keep Developers Motivated

Although identity is important to the success of a customer-facing application, developers typically don’t enjoy building identity and security infrastructure. Although it’s a high-risk area and often fraught with complexity, user management is perceived as mundane, and developers would rather work on features tied to core product differentiation and cutting-edge systems. The high overhead associated with implementing user security can be especially demotivating—there is a great deal of risk, and much conflicting guidance. On the other hand, developers perceive working with modern REST-JSON API services as interesting and accessible.

Deliver High Scalability and Reliability

When user management fails, it’s like locking the door to your store before closing time. If the login experience fails due to a lapse in availability, end users won’t know or care why—but their perception of your organization and your brand will suffer. The level of consumer load is unpredictable, and marketing departments do not always know or share when a promotion will drive an influx of users. If you decide to manage this yourself, you have to be confident in your team’s ability to offer multiple nines of availability, and scale easily as the user base grows. You must be prepared to provide double or triple redundancy in your datacenter or in collaboration with an infrastructure-as-a-service provider. You will need to provide for seamless upgrades and maintenance to ensure uninterrupted service. Companies who take on these nontrivial responsibilities often find the maintenance overhead unmanageable. An outside user management service provider can completely remove the operational headaches.

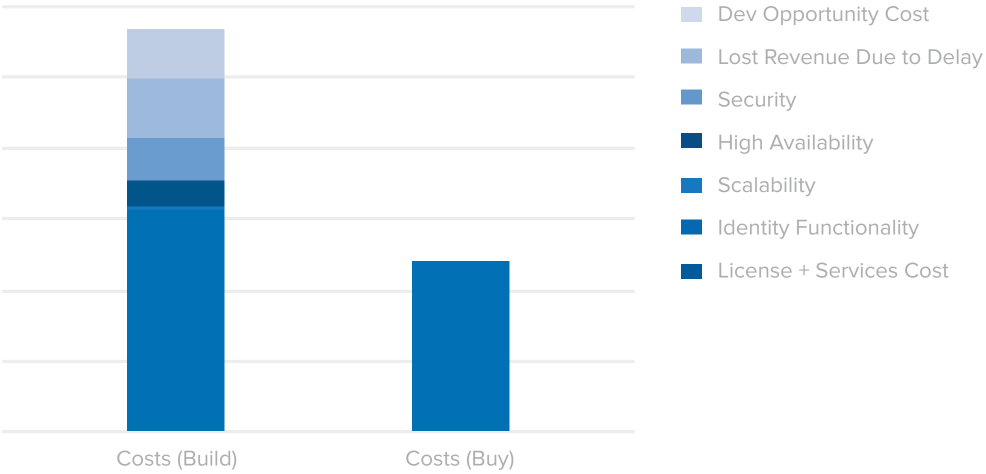
> “
>
> Facilitating integration across the ecosystem, making sure identity persists across systems, and having identity be the central way we’re relating to the customer, with a high degree of reliability and availability—that was really important to us.
>
> James Fairweather
> Senior Vice President of E-Commerce and Technology, Pitney Bowes

Summary

Development teams have increasingly turned to pre-built tools to offload some of the burden of application development. Identity and access management presents developers with a broad range of challenges that a trusted identity layer can help offload easily. This is a sound strategy for companies of all sizes that want to accelerate time-to-market, reduce costs, focus development teams on core functionality, and realize a host of other benefits. While a few organizations still hesitate to embrace API services, this is largely based upon misperceptions that should be readily dispelled in scoping out a project. While developers have historically balked at giving up portions of the stack, they will readily do so when a solution is proven out such as Twilio for communications and Stripe for payments.

In many ways, identity should be treated like a tattoo. Embedding a DIY solution limits your ability to scale into the future. Because identity is so critical to your application stack, choosing the right solution from the start is paramount.

Build vs. Buy Total Cost of Ownership Comparison



The Okta Identity Cloud

Purpose built for the modern era, the Okta Identity Cloud enables organizations to deliver secure, frictionless digital experiences for their workforces, partners, suppliers, and customers. It's a modern, secure identity layer that can serve as identity building blocks for your mobile or web applications to accelerate the time-to-market of your digital projects:

- Embeddable Authentication—Provide your users a frictionless, secure experience. Leverage Okta's prebuilt UI widgets for common user flows such as login, registration, and password reset or build a completely customized experience with Okta's APIs.
- Embeddable Authorization—Control which APIs your users and developers have access to using Okta's API Access Management. Customize claims and scopes, as well as insert external attributes using Okta's token extensibility.
- User and Policy Management—Manage your users and security policies programmatically via APIs or from our userfriendly admin console. Create single sign-on (SSO) experiences and manage the user lifecycle with automated onboarding and offboarding.
- Developer Efficient—Ranging from "no-code" to "pro-code", get started with minimal development resources using Okta's hosted customization tools, or use Okta's SDK and REST API to build with the programming language and framework of your choice.
- Production Ready—Scale with confidence with 99.99% availability SLA*. Monitor potential security threats in realtime with the admin System Log. HIPAA, FedRAMP, GDPR, and PSD2-compliant.
- Okta Integration Network—An entire ecosystem supporting your development efforts. Integrations include 5,000+ pre-built connectors for SSO to applications, API gateways, IaaS, identity proofing, and application delivery controllers.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 application integrations, Okta customers can easily and securely use the best technologies for their business. To learn more, visit **okta.com**.