Whitepaper

Setting the Bar for Enterprise-Grade Identity

Benchmarks to build and manage secure SaaS apps for the future

What's in store

Introduction

To build a great SaaS application, first consider your users. Who are the people who will interact most closely with your app? What are their needs and objectives?

One critical user is the end customer—the person who will rely on your app every day to get work done, solve problems, and achieve business goals. Regardless of their role or industry, they'll almost certainly need your app to be easy to use, powerful, and secure.

But there's another important user that app builders need to consider: the IT administrator.

This key stakeholder will be responsible for implementing your SaaS application within their organization. They'll not only want to make sure that your app meets their team's needs, but that it also fulfills enterprise-ready criteria for stability and security. And as new threats continue to emerge, their requirements will likely grow more rigorous and complex.

As a SaaS app builder, how can you deliver solutions that satisfy both of these users today and meet the evolving security challenges and industry standards of tomorrow?

In this whitepaper you'll discover six fundamental benchmarks to help you build SaaS apps that are enterprise-ready for both your end customers and the IT admins who support them. These benchmarks include:

- Passwordless Authentication
- Single Sign-On
- Continuous Access Evaluation
- Provisioning
- Authorization
- Simplified Setup

Read on to learn more about each of these benchmarks—what they are, why they matter, and how you can take action on them to build modern, enterprise-ready Identity into all of your SaaS applications.

Passwordless Authentication

+80%

More than 80%
of hacking-related breaches this year used stolen and/or weak passwords.

Passwords have long been the most common way that enterprise users access apps. But they're inherently weak and persistently hard to eliminate. Fortunately for those building enterprise-ready apps, the FIDO Alliance, an association committed to providing open authentication standards, has developed more secure, convenient alternatives. These new credentials, often called passkeys, use public-key cryptography and are bound to a specific domain. They have the potential to eliminate passwords and whole classes of attack vectors.

Passkeys replace per-site passwords with a single biometric or PIN and rely on the user's own device for authentication. Not only do passkeys improve security, they also streamline the user's login experience, which can be as seamless as tapping a button—no usernames and passwords required.

Why it matters: It's no secret that passwords aren't secure. More than 80% of hacking-related breaches this year used stolen and/or weak passwords. What's more, phishing attacks, which are often used to steal passwords and other credentials, are on the rise. Passwords and multi-factor authentication using one-time passwords (OTPs) or push notifications are phishable and pose serious risks, such as account takeover. To create enterprise-ready apps, builders need to adopt phishing-resistant authenticators and move away from passwords.

Take action: All major operating system and browser vendors are rolling out updates that will make passkeys more widely available. To take advantage of this, those building apps for the enterprise will need to implement single sign-on and provide ways for admins to verify that users authenticated with a passkey or security key. They'll also need to ensure that their app supports WebAuthn, a credential management API that allows web apps to authenticate users with passkeys instead of passwords.

Resources:

FIDO Alliance

W3C Recommendation

OpenID Connect Extended Authentication Profile

Our Take on PassKeys, Auth0

Single Sign-On

Single sign-on (SSO) allows enterprise users to quickly and conveniently access all of their approved apps by entering their credentials only one time. From an enterprise IT admin perspective, SSO centralizes authentication through a single Identity provider, simplifying the management of user access policies and lifecycles.

Why it matters: SSO is a critical component of an enterprise's security strategy—with fewer credentials, there are fewer opportunities for bad actors to steal them. What's more, app builders today are unbundling traditional web applications into separate backend APIs accessed through web and mobile app frontends. SAML, the traditional protocol for implementing SSO, lacks features needed to secure APIs from being accessed by third-party applications. This puts enterprises at risk. By ensuring apps are SSO configurable, builders can head off enterprise security concerns and ease the burden on IT admins.

Take action: App builders should adopt OpenID Connect (OIDC), a simple Identity layer that works on top of the OAuth 2.0 framework. OIDC supports SSO for both web and native applications. And because it is built on OAuth 2.0 protocol, it also provides the capabilities to manage and secure API access.

Resources:

OpenID Connect

OAuth 2.0

OAuth 2.0 Simplified

Continuous Access Evaluation

While authentication is essential for securing access, it is also a single point-in-time event. After authenticating, enterprise users have ongoing access to an application for the duration of their session. However, the assurance level decays over time, and the app must re-prompt the user to log in. Continuous access evaluation regularly evaluates access policy to minimize the decay in assurance and the number of times users are prompted to authenticate.

Why it matters: For enterprises, continuous access evaluation eases the tension between security and the user experience. For example, if an enterprise user logs into their company's email app with SSO, they'll want the app session to last as long as possible. It's more convenient to authenticate once every 24 hours than every few hours. But the enterprise's Identity provider (IDP) might demand more frequent re-authentication to maintain high levels of assurance. Continuous access evaluation balances these interests by enabling enterprises to maintain session security while minimizing repeat logins.

Take action: App builders should support single logout (SLO), allowing IDPs to terminate active sessions during security events. This is a simple step toward allowing IDPs and apps to jointly manage sessions. App builders should also begin implementing Continuous Authentication Protocol (CAEP), which allows for more granular session control. For instance, the access associated with an existing session could be lowered, rather than terminated. This enables long-lived sessions with step-up authentication only when necessary.

Resources:

OpenID Connect Back-Channel Logout 1.0

OpenID Continuous Access Evaluation Profile 1.0

Security Events (Secevent) Working Group

Shared Signals and Events – A Secure Webhooks Framework

NIST 800-63 Digital Identity Guidelines

Provisioning

Identity provisioning automates lifecycle operations as employees join, move within, or leave an organization. These operations ensure that employees can access apps needed to do their job and that access is revoked when necessary.

Why it matters: At an enterprise level, provisioning can involve highly complex onboarding and offboarding processes. Different user groups may require vastly different levels of access, and IT admins must quickly revoke access for users who leave the organization. Ensuring that employees have access that matches their roles and responsibilities is crucial for meeting basic compliance and security requirements.

Take action: App builders should ensure their product supports the System for Cross-domain Identity Management (SCIM), an open standard for creating, updating, and deleting user accounts and identifying information across systems and applications. They should also consider implementing APIs for all their customers to automate business processes.

Resources:

Understanding SCIM

Authorization

Authorization is the process of determining who has access to what. It is closely related to authentication, which is a prerequisite for determining who the user is. Enterprise organizations need to be able to accurately assess user access privileges to audit systems and achieve regulatory compliance.

Why it matters: Application access policies can be managed centrally via SSO. However, the applications themselves protect a variety of resources with various permissions. Understanding these fine-grained permissions and the access individuals have requires deeper integration than just SSO.

Take action: App builders should be designing authorization models with the expectation that external customers will need insights into how they are applied. Standards for how enterprise IDPs and B2B SaaS applications integrate are nascent, and Okta will be driving innovation here through our integrated Workforce Identity Cloud and Customer Identity Cloud products.

Resources:

OpenFGA

Workforce Identity Cloud

Customer Identity Cloud

Simplified Setup

For enterprise admins, configuring and managing an Identity system can be an arduous task. Adding a new application or API is typically a manual process that involves copying and pasting sensitive credentials. When things go wrong, as is not uncommon, diagnosing the issue can prove challenging.

Why it matters: For enterprises, the time-to-value of a new app is an important metric. Manual processes lead to delays in procurement, increasing time-to-value and decreasing customer satisfaction. Additionally, enterprises need to maintain security best practices, such as frequent key rotation, which depend on automation for reliability.

Take action: App builders should implement support for Fast Federation, which allows an enterprise admin to connect their IDP to the app with a few clicks. Once setup is complete, the IDP and app have a programmatic channel to manage configuration, allowing for automated changes and key rollover.

Resources:

Fast Federation

Get Started

Enterprise Identity is rapidly evolving, and now is the time to prepare for the changes. Each of these benchmarks strengthens the security posture of an app and its enterprise customers, while simultaneously improving the end-user experience.

Ready to get started? Learn how the Okta Integration Network can help you build and distribute enterprise-grade apps.

Whitepaper

Setting the Bar for Enterprise-Grade Identity

okta

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