

First Report on the State of Homegrown Authentication Shows 50% of Developers Prefer Local Testing

New study reveals a split in development approaches, with many teams opting for downloadable software over multi-tenant SaaS for authentication

BROOMFIELD, CO, UNITED STATES, April 2, 2025 /EINPresswire.com/ -- This inaugural [State of Homegrown Authentication Report: 2025](#), sponsored by [FusionAuth](#) and [Cloudelligent](#), is the first to dive into the experience and tech stack of the teams building and maintaining their own login experience. The burgeoning Customer Identity and Access

Management (CIAM) market, which effectively outsources the login experience, has generally ignored the tools, technologies, and trends shaping homegrown authentication solutions. This report highlights a key group of developers that remain committed to building their own authentication solutions—often for greater control, security, or flexibility.

“

It would be a mistake to forget the needs of those building login themselves today; we should instead be sharing best practices & tech stacks in tandem, to support the development of better dev tools.”

Brian Pontarelli, CEO and Founder of FusionAuth

The findings uncover a clear divide between what DIY authentication teams want and need versus what the dominant multi-tenant SaaS CIAM market offers, with at least 50% of self-hosted authentication teams preferring downloadable software over cloud-only solutions. This preference reflects a desire for greater control over deployment environments, as well as concerns about data residency and security risks associated with multi-tenant SaaS models.



First Report on the State of Homegrown Authentication Shows 50% of Developers Prefer Local Testing

The CIAM industry grew quickly between 2015 and 2020, fueled by developer influence and the

push for digital transformation. But plenty of teams are still building and managing their own authentication systems and doing it successfully. Companies like GitHub, Google, and GitLab prove that in-house authentication can scale. Yet, most industry reports ignore these developers, leaving them without insights into how others are tackling the same challenges.

“We have to remember that, as an industry, no more than 10 years ago, we were all building login ourselves. It would be a mistake to forget the needs of those that are building login themselves today; we should instead be sharing best practices and tech stacks in tandem, to support the development of better dev tools,” says Brian Pontarelli, CEO and Founder of FusionAuth.

The State of Homegrown

Authentication report paints a clear picture of the teams building their own login systems—from the mix of third-party libraries and auth servers they use (or don’t) to the people dedicated to the task. Only 30% lean on external help like third-party auth servers or libraries, while the rest either run their own auth server or build everything from the ground up. And they’re not handing this off to just anyone—60% of teams say their best and brightest are leading the charge.

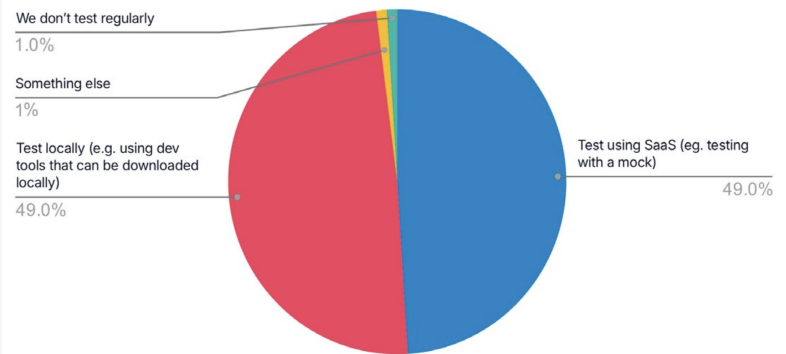
The survey also found that passkeys are a polarizing feature. The same number of respondents felt like experts as those who felt completely unfamiliar with them. And when it comes to the biggest advantage and biggest challenge of running authentication in-house, the answer is the same: security. While teams value having full control, 20% reported experiencing a security breach in their homegrown auth system.

“As organizations navigate the complexities of authentication, they require solutions that offer both flexibility and security. This report underscores a critical reality—many development teams still prefer self-hosted authentication for the control it provides. At Cloudeelligent, we empower businesses to build and optimize cloud-native architectures that support their unique authentication needs, ensuring they maintain agility without compromising security.” – Qasim



Cloudeelligent partnered with Fusionauth on the inaugural State of Homegrown Authentication report

Chart 20. Which of the following types of software do you prefer for your testing environments?



The inaugural State of Homegrown Authentication report found that 1/2 of teams prefer testing locally

Akhtar, CEO of Cloudelligent.

Since around 2020-2022 outsourcing CIAM has meant mostly moving into a multi-tenant SaaS model, with no option for self-hosting or downloading locally. This study shows that those solutions risk alienating at least 50% of the providers that might be looking to outsource their authentication moving forward.

To see the entire tech stack of teams building their own authentication, including the authentication libraries that are easiest to implement and maintain, the top programming languages, protocols, and CI/CD frameworks, download the full report here:

<https://fusionauth.io/tech-papers/homegrown-authentication-report-2025>.

About FusionAuth

FusionAuth is the only downloadable Customer Identity and Access Management (CIAM) platform with an enterprise-grade, hybrid deployment model for diverse development pipelines. Trusted by over 450 global organizations, FusionAuth provides customers of any size with a single-tenant VIP suite, the option to download and run anywhere, world-class support, and no hidden costs regardless of scale.

About Cloudelligent

Cloudelligent is an AWS Advanced Consulting Partner that delivers end-to-end solutions for businesses looking to accelerate their journey on AWS. With a diverse team of AWS-Certified Solutions Architects and Engineers, Cloudelligent helps organizations architect, migrate, optimize, secure, and manage their workloads to achieve desired outcomes and expand into new global markets. They empower companies to innovate faster and maintain their competitive advantage by leveraging AWS services. To learn more, visit cloudelligent.com and follow them on LinkedIn.

Daniel Delson

Magnitude, Inc.

daniel@magnitude-growth.com

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[Other](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/799073004>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

