Whitepaper

The real cost of an in-house Identity solution

okta

Introduction

While building Identity in-house is an option you've no doubt considered, the costs of doing so can be astronomical if the right strategy isn't set in place. For example, have you ever had your engineering team build out an Identity solution just to have the stack or regulations change within 3 to 6 months? Don't worry – you're not alone.

And while not a unique phenomenon in tech, attack vectors are constantly evolving – meaning fraud prevention is more mission critical than ever before and even more difficult to address. Plus, when it comes to compliance for handling customer data and protecting your services, organisations have limited lead time to deploy updates to their stack.

Though having the right Customer Identity solution in place can solve all these issues, building it in-house can often create more problems than it solves. Here are some key points to help explain why:

The cost of having a team solely dedicated to Identity

DevSecOps are the gatekeepers for all the MDR (Managed Detection and Response) and Extended Detection and Response (XDR) needs of an organisation. But typically, organisations who are working with legacy systems often leave it to the engineering org[1] to determine the RACI for application engineers and security practitioners.

Often, Identity technology ends up getting caught in the fray because DIY Customer Identity solutions are usually built at the application-level. Customer Identity also puts a strain on DevSecOps because additional collaboration across different engineering teams must be done to ensure that their consumer applications and points-of-service deployments are secure.

As a result, collaboration comes at a cost to organisations – and without automated access for discrete provisioning, role-based access control (RBAC) and just-in-time manufacturing (JIT), deployment times are much longer, and monitoring is not comprehensive.

In addition to the above, DevSecOps is becoming more agile – and acceleration to the Cloud requires strategic investment in the right tools[2] for risk assessment across different processes and frameworks in the Continuous Integration/Continuous Delivery (CI/CD) pipeline.

Optimised cloud environments, however, can offer an improvement of about **38%** in maintenance productivity, and infrastructure cost savings of about **29%** for migrated applications[3]. This is significant capital that organisations can use to re-invest in their core operations.

[1] Why your security risk management program should include legacy systems, Infosec Institute

[2] The best IAM practices for DevOps, develops.com

[3] Clouds trillion dollar prize is up for grabs, McKinsey

The rising cost of technical debt

Implementing streamlined authentication with strong security standards across multiple applications and resources has no endgame. Manual user provisioning not only requires heavy operational investment, but, for more complex or dynamic systems, it can result in the wrong access—as in, your users might be able to access more than they should.

It's also easy for an engineer to collect too much data in-payload or write a claim that doesn't capture access specificity, which opens organisations to malicious activity.

Alongside the risk of human error, managing Customer Identity in-house also requires consistent maintenance and good housekeeping. The larger the digital footprint, the larger the attack surface[4], and all a bad actor needs is access to just one account to cause a data breach – and with quantum computing on the horizon[5], in-house encryption services are even more vulnerable to data theft.

Yet, by outsourcing the responsibility of Customer Identity to a trusted provider, organisations can quickly gain peace of mind with well-architected security protocols that safeguard against malicious AI activity.

[4] Securing The Future: The Most Critical Cybersecurity Trends Of 2023, Forbes

[5] A game plan for quantum computing, McKinsey

Compliant Data Processing is Cookieless

We are all learning more and more about how our personal information runs the Internet, and technology, regulations, and users are more engaged in changing current data practices to be more transparent and consumer moderated.

Third-party cookie collection has been the cornerstone for personalisation but has inherent data privacy concerns, particularly when it comes to user consent and data ownership. However, soon, we will see a phasing out of cookies[6] – and this has many implications for how businesses are currently gathering and exchanging their customers' information, as well as building their customer profiles.

Today, users are becoming more discerning about what applications they share their data with[7], and regulations are supporting the consumer by pushing organisations to make an active effort to develop brand trust with their customers through a cookieless strategy.

> 27% of technology leaders say ensuring data collection processes comply with privacy and security regulations is their #1 challenge[8]
>
> **– Kantar/Okta research**

To ease these pains, many organisations now choose to outsource their Customer Identity solution build to trusted providers that offer cutting-edge out-of-the-box features. Progressive Profiling, for example, gives your users a way to tell you what they want you to know about themselves, without the cookies, and without the headache of pouring even more engineering resources into maintaining compliance requirements.

[6] The Slow Death Of Third-Party Cookies, Forbes

[7] The mismanagement of user consent data and its consequences, iapp

[8] Okta's Future is CIAM: Insights from APJ leaders

Building consumer loyalty at the speed of the market

From the outset, it seems like a simple value-proposition: the less time it takes for your customer to login and go to check out, the more likely they will be to convert[9] – but there are a lot of caveats for what is considered friction and how friction is securely reduced for a user at the authentication and authorisation stage.

Brand trust is not just about collecting zero-party data at sign up and login, but pulling out all the stops to make sure your customers benefit from a secure login experience[10], too.

While in-house Identity does little to solve these challenges, organisations that have invested in cloud Customer Identity solutions are already benefitting across the board. As well as being able to offer tailored customer experiences[11] that give users the choice of how they authenticate, these solutions also comply with all the latest privacy and security standards, increase conversions with better user experiences, and empower engineering teams to go forth and innovate.

[9] Conversion Rate Optimization – It's a Journey, Not A Destination, Customer Think

[10] Access management must get stronger in a zero-trust world, Venturebeat

[11] The Benefits Of Passwordless Authentication And How To Choose The Right Method, Forbes

Why Okta?

Customer Identity is about embracing change and adapting to new frameworks, and organisations that understand what their customers need before they need it, and find ways to ship their vision fast, outpace their competitors.

A good Customer Identity solution like Okta not only balances innovation and security, it also gives you the ability to perform one-click integrations for your multiple applications and services as you grow. With features such as breach notifications, layered attack protection, and orchestration available from day one, we can also help you to better secure your applications and services as well as to learn more about your customers.

Finally, with the latest standards in Identity and security built-in, Okta Customer Identity Cloud offers a complete solution that has already helped many organisations innovate at pace while providing a safer, swifter, and more convenient digital experience for their consumers.

For a more in-depth look at how Okta's Customer Identity Cloud can help your organisation, check out our Build vs Buy whitepaper.

Whitepaper

The real cost of an in-house Identity solution

okta

Australia Headquarters
80 Pacific Hwy
North Sydney NSW 2060
(02) 8318 7677