Whitepaper

The future is CIAM: Insights from APJ leaders

okta

Introduction

Over the last 36 months, we have witnessed an evolution in the way businesses deliver digital customer experiences. With more than half[1] of customers now preferring to do most of their shopping online, organisations must re-evaluate how they engage with their customers and maintain relationships of trust.

The global shift to remote and hybrid working has also caused major disruption. As well as ensuring each employee has swift, universal access to the apps and tools they need to work, gaps in remote work security and the rising costs of managing data breach mitigation[2] have created many new challenges for IT and Security leaders.

On the B2C side, organisations want to earn consumer trust, but aren't sure how to streamline the digital experience to optimise for conversion while also safeguarding their customer's personal data. On the B2B side, organisations want to upgrade their microservice scaffolding to the cloud to better collaborate with their vendors, suppliers, and partners – but they don't want weak passwords to put their systems at risk. And all organisations want consistent authentication and authorisation across multiple applications and services.

To better understand the role cloud Identity plays in solving these challenges, and how Digital Native Businesses (DNB) and Independent Software Vendors (ISV) technology leaders in APJ want to approach it, Okta recently commissioned Kantar to conduct a detailed study[3]. Here are some of the key findings.

[1] State of the Connected Customer, Salesforce

[2] Enterprise security solutions, IBM

[3] Okta APJ DNB/ISV Research

UX vs security: Why not have both?

Strong security standards have been historically difficult to assess and implement. Creating tailored authentication policies from scratch to manage your users' access privileges requires heavy engineering investment, and organisations do not want to hinder their users with policies that are too stringent because they lack the resources needed to create an adaptive authentication framework.

From the survey we can see that:

28% of respondents struggle to balance a streamlined digital experience with security and are looking for solutions.

55% find it difficult to compete for resources with other high priority security initiatives in the organisation.

40% of technology leaders interviewed choose to minimise security barriers to streamline the digital experience.

60% of organisations are using two-factor authentication, and almost 9 in 10 organisations are using at least one authentication method to secure the digital experience of their users today.

When asked about the main methods used to secure the digital experience today, respondents prioritise two-factor authentication (60%), password strength requirements (59%) and CAPTCHA (54%). Almost 9 in 10 organisations are using at least one of these methods to secure the digital experience of their users today.

Balancing the scale between security and usability

As the Internet has matured, so too have the attack vectors – rendering password-only applications a liability. Yet, despite the common perception that implementing Multi Factor Authentication (MFA) places huge strain on engineers and massively inconveniences the customer – the right MFA and passwordless[4] solutions can significantly improve overall security posture and reduce friction across the board[5].

For B2Cs, passwordless logins can quickly eliminate password fatigue – allowing your organisation to benefit from higher conversion rates[6]. Reducing friction during the authentication process also leads to significant improvements for the bottom line – with around 8 in 10 B2C organisations saying simpler registration processes increase their sign-up, conversions, and customer retention rates by at least 50%.

Reducing friction during the authentication process would likely lead to significant improvements:

- About 8 in 10 (79%) estimate at least a 50% improvement in sign ups/registration rate.
- Almost 8 in 10 (75%) estimate at least a 50% improvement in conversion/check out rate.
- Almost 8 in 10 (76%) estimate at least a 50% improvement in customer retention rate.

Also, by investing in Identity as a Service (IDaaS) products that have configurable low-code/no-code authentication policies, it's easier for developers to set up and can provide an even more seamless experience for your users. This is because you're giving them options to authenticate, with a level of security that makes sense for their session.

By giving users simple authentication choices, you can cut down the amount of time and steps it would take to come up with yet another password and possibly abandon their session or checkout. For example, being able to conduct device detection and authenticate with FaceID is a tailored approach to accommodate that individual's digital comfort and ease, improving the Customer Experience (CX), which fundamentally develops brand trust[7].

[4] Annoying Password Rules Actually Make Us Less Secure, Wall Street Journal

[5] How CIOs can drive Identity-based security awareness, Venturebeat

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

[7] Building better experiences with passwordless authentication, Harvard Business Review

How can brands build trust with data privacy in a Cookieless future

More than 50% of organisations indicated that the #1 perceived benefit of having a complete customer profile is to build better customer-centric capabilities, develop effective marketing and loyalty programs, predicting future needs and requirements, and/or providing tailored experiences for customers.

Third-party cookies have been the path of least resistance for organisations to gather customer engagement and insights – but this came at a price. With all the gathering and exchanging of user data across many platforms and services, data privacy was compromised. And while personalisation drives consumer loyalty[8], brands that over-rely on cookies actually turn off their consumers[9].

Overall, the number one benefit of having complete customer profile information is to build better customer centric capabilities (62%) but it is also important for developing effective marketing and loyalty programs (60%), predicting future needs and requirements (59%) and providing tailored custom experiences for customers (58%).

Identity is the key to great customer experience

Due to the downstream effects of identity and privacy changes from Google and Apple[10], potential markets are already increasingly operating in cookieless environments. In fact, twenty-seven percent of CTOs interviewed said their greatest challenge is to address the ramifications of cookieless and the impact on gathering customer insights and maintaining good CX.

Considering this, organisations that don't buy into the urgency of the shift to cookieless and fail to strategically invest in upgrading their applications will experience detrimental losses to their bottom-line quarter after quarter[11]. When third-party cookies are phased out, B2Cs should create a dialog[12] with their consumers. Engaging users for zero-party data with approaches such as Progressive Profiling also gives your users a chance to volunteer what they want you to know about them.

[8] How to Prepare for a Cookieless Future, IBM

[9] Why digital trust truly matters, McKinsey

[10] Three steps for marketers to prepare for in a cookieless world, Gartner

[11] Brands that rely too heavily on third-party cookies are leaving money on the table today, risking long-term business harm, Adobe

[12] As Third-Party Cookies Fade, Brands Get Personal, Forbes

Amongst those using an in-house solution, 62% of DNBs are more likely to consider moving to a SaaS based identity service because of evolving regulation and compliance around identity and privacy.

According to the survey, the main challenge for over half of respondents was developing the infrastructure to gather and meaningfully use customer profile data with their current customer identity solution. For this reason, investing in a customer identity solution that features both CDP and CRM integrations will be essential to continue to develop rich customer insights and develop brand trust[13].

But brand trust doesn't stop at going passwordless or cookieless – it's also about being transparent about how you're consuming user data[14] and giving your users the power to control the collection process. Users want to know how you're using their data[15], and when, and want to be able to control how it's being collected, via consent that can be tracked, changed, and revoked.

Although 56% of CTOs agreed that privacy regulation compliance was vital, a further 64% agreed that guarding customer trust regarding data collections was just as important. By choosing the right customer identity solution, your business can maintain data privacy compliance more easily and help build customer relationships by giving users a choice of what information they share.

A customer identity strategy that is cookieless and data-privacy-forward also means that your customers will be more open to participating in loyalty programs and reactivation with special offers[16] – helping you understand them better and giving you the information needed to keep them coming back to your business in future. A good CIAM solution keeps your customers coming back.

[13] 5 Areas Where CIAM Is More Than An IT Responsibility, Forbes

[14] In better customer experiences we trust, Adobe

[15] **[16]** As the cookie crumbles, three strategies for advertisers to thrive, McKinsey

Should I build or should I buy Identity?

Many organisations went through digital transformations in recent years[17] to address an influx of user activity to stay competitive in the market. But those that rushed to the Cloud using the same strategies used to build in-house solutions[18] ended up with a different set of road blocks. Multiple SaaS vendors and inefficient shift-and-set migrations resulted in increased friction for employees and partners who then had to manage their services across multiple interfaces. This caused hesitation in the market to buy third-party solutions to meet their needs.

According to the survey, about two-thirds of organisations in APJ are still using an in-house customer identity solution. Yet, building in-house customer identity infrastructure that connects all your upstream and downstream services while maintaining a private and secure session for your customers comes at a significant cost, to both your engineers and your organisation:

- **1/3** of Product leaders said they are most concerned about developer efficiency.
- Organisations interviewed estimated the cost to be at least **6 FTEs** to implement identity in-house.
- **52%** of DNBs have multiple apps with different identity services underpinning them.
- **38%** of DNBs view an in-house identity service as a blocker to a microservices architecture.

Despite this, 62% of respondents in the survey were concerned about migration complexity, in other words, the potential cost to dismantle brittle infrastructure and workarounds without 1:1 solution immediately available out-of-the-box. To solve these challenges, organisations, especially enterprise, need to fundamentally change their approach to building software.

[17] Why Do Companies Need Digital Transformation? Forbes

[18] Why you should pay attention to the rise of SaaS paltfroms, Forbes

What are the benefits of using Identity-as-a-Service?

- **Automates** engineering-heavy operations to streamline your Identity infrastructure, improve compliance, and most importantly, guard your digital assets[19].
- **Increases visibility** over your data, ensuring you can easily see who is accessing what from a single centralised location.
- **Simplifies privacy management** to ensure your customer and employee data remains secure and protected.
- **Strengthens security** and defends your services from attacks[20] by eliminating threats.
- **Improves the customer experience** by eliminating login friction and strengthening security without impacting usability.

The key is to set your employees up for success with SaaS solutions like Okta that offer orchestration tools to solve their problems and reduce context switching by providing a single-pane view for all your services. Businesses that have already leveraged cloud data centres and SaaS solutions that address personnel efficiency have also experienced massive savings[21] – and the right Customer Identity solution also helps you to better secure your applications and services as well expand your business.

That's why Identity solutions such as Okta already have partnerships with common Cloud Providers (e.g. AWS, GCP, and Azure) to make distributed cloud an easy transition, and help ISVs maintain high SLAs and optimise personnel resource investment[22].

Moving architecture to the Cloud with modular services such as IDaaS adds commercial value for both B2Bs and B2Cs by increasing business resilience and agility, reducing cost, improving partnerships, and making room for more innovation[23]. Technology that supports a healthy Digital Immune Systems (DIS)[24] promotes business outcomes by accelerating product delivery of vertical offerings and tapping into new virtual markets.

By offloading Identity to an IDaaS like Okta, you can connect the dots between your applications and services, accelerate developer velocity with simplified integrations and orchestration for complex use cases. IDaaS investment ensures prime uptime for your customers, helps you get ahead of your competition, and protects your business.

In other words, with solutions such as Okta Customer Identity Cloud, you get more innovative security measures for less internal technical investment, so you save on resources and expedite time to value.

[19] Why you need a Zero Trust cybersecurity plan, Forbes

[20] IDaaS – Identity at the Heart of Security, Bloor Research

[21] The World Has Changed: So Must Cybersecurity, Forbes

[22] Building a cloud-ready operating model for agility and resiliency, McKinsey

[23] Top Technology Trends, Gartner

[24] Glossary, Gartner

Conclusion

Your CIAM strategy must balance all the organisation requirements that are impacted by customer Identity—and IDaaS optimises for security, UX, and resource efficiency:

- MFA and passwordless is more secure and reduces friction, which significantly increases user productivity and conversions. IDaaS gives your engineers an easy way to implement policies that are tailored to your users.
- Customer Identity means cultivating a transparent, zero-party relationship with your consumers and adapting to new topographies. Organisations that prepare for cookieless now by investing in IDaaS with tools such as Progressive Profiling will outpace their competitors in potential markets.
- With Identity as your perimeter, investing in a CIAM solution like Okta and implementing a successful SaaS migration is all about automating manual processes and providing a single source of truth for your personnel. CIAM investment drives consumer value, business value, time to market, and the bottom line.

Organisations that have embraced IDaaS save on IT resource investment and have the fiscal freedom to focus on core product development, and ultimately have better customer and partner relationships.

Why choose Okta?

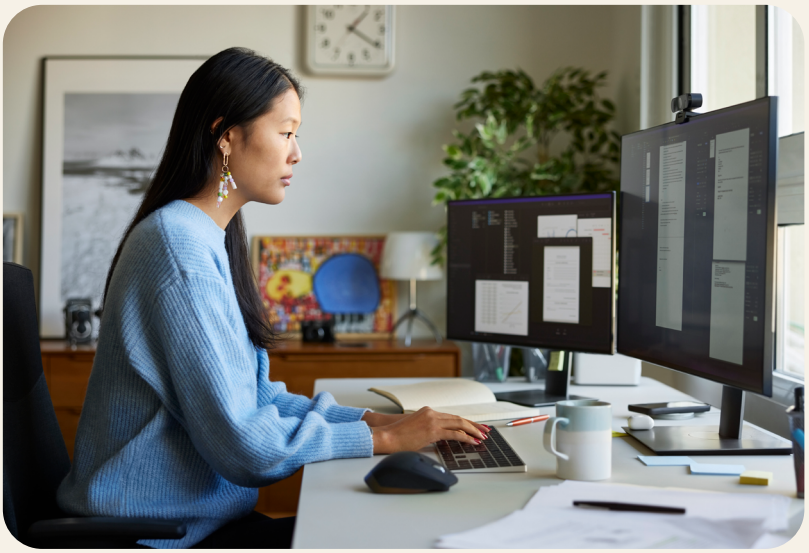
When it comes to CIAM, Okta Customer Identity Cloud (CIC) is not just another out-of-the-box solution for Identity.

Okta CIC is an intuitive platform for organisations to build out their own security posture with low-code/no-code orchestration to optimise developer efficiency and save on engineering resources.

With advanced integrations at the click of a button, we help organisations to deliver streamlined, personalised experiences for their customers while helping you adhere to data privacy and consent regulations and requirements to build brand trust, at speed.

With Okta CIC, you can reclaim your time—time that can be used to focus on your own product's innovation strategy, and be the next big thing in your industry.

Get in touch



Whitepaper

The future is CIAM: Insights from APJ leaders

okta

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