computing
research

# RESEARCH PAPER

# Is convenience still king? Why good user experience and security must reign together in CIAM after the pandemic

April 2021

Sponsored by
okta

## CONTENTS

# Introduction

A year of pandemic lockdowns has pushed millions of customers towards online, cloud-based, and mobile services, including buyers who would normally prefer bricks-and-mortar options.

For those who had yet to be convinced, this sudden acceleration of what had been a steady drift into the cloud has proved the concept of clicks either replacing, complementing, or supplementing bricks (as necessary). Not just in obvious sectors such as Retail and Financial Services, but also in Education, Training, Government, Healthcare, Entertainment, and others where online activities have usurped traditional, in-person alternatives – out of necessity in many cases.

Even once this crisis has passed, it is likely that the speed and convenience of mobile apps, cloud platforms, and digital outlets will leave lasting behavioural and preference changes in their wake, though many organisations and their customers will doubtless relish the opportunity for face-to-face contact once again.

But the crisis has also created a giant pool for sharks to swim in – cyber criminals who scent opportunity in unwary users and providers. This affects customers themselves, along with every organisation that needs to authenticate, manage, and protect users' activities and data.

Robust data management, encryption, password policies, multi-factor authentication, risk management, scalability, and compliance are just some of the must-haves for every organisation – both now and in the post-pandemic world that IT leaders should be planning for. The penalties for any failure could be severe, both in terms of legal liability and reputational damage.

This white paper, featuring exclusive *Computing* research, uncovers what leaders should be prioritising when it comes to customer identity and access management (CIAM). It reveals the results that some are already seeing from their customer initiatives and explores how the accelerated shift to digital has been influencing their activities.

# Low friction, high advantage

So, what does it take to be king of CIAM and to secure trusted customer relationships? And how has the pandemic shifted internal and external priorities?

These are big questions for IT leaders, because users increasingly demand digital experiences that don't get in their way, but also reasonably expect to have their preferences recognised and their data protected. The law expects that data to be protected too.

So, there are tensions whenever low friction meets high risk. On the one hand, users need to be authenticated and to have their data secured, but on the other, they don't want to keep jumping through unnecessary hoops to access what they may regard as a commodity service. Get this part of the experience wrong, and customers may click away to your competitor.

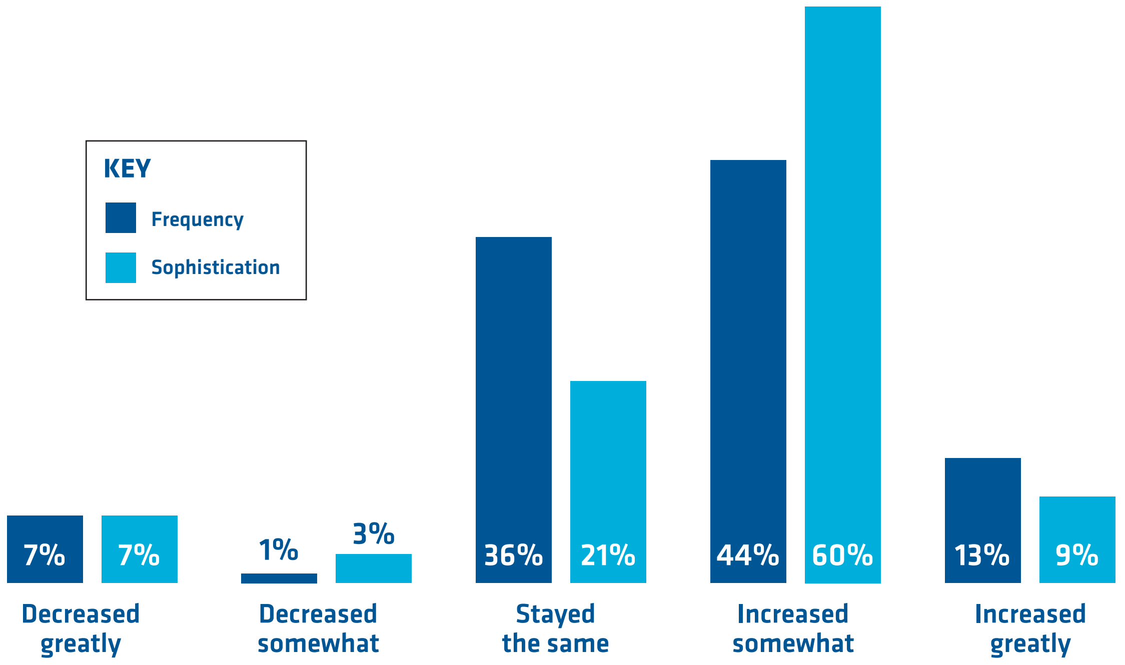
Put another way, customer sign-in solutions need to provide a good user experience, while reliably authenticating both the user and their device. But securely managing identities on websites, cloud platforms, and digital services while providing a good user experience (UX) can seem like mutually exclusive aims.

And that's not the only issue facing IT leaders. The need for security policies, protocols, and technologies to adapt to the 'new normal' of the Covid world is clear.

# Balancing competing demands?

A survey of 150 IT leaders in medium to large organisations across every sector of the economy, all of whom are involved in CIAM strategy or implementation, found 57 percent reporting that cyberattacks on corporate systems have increased, either significantly or somewhat, during the pandemic.

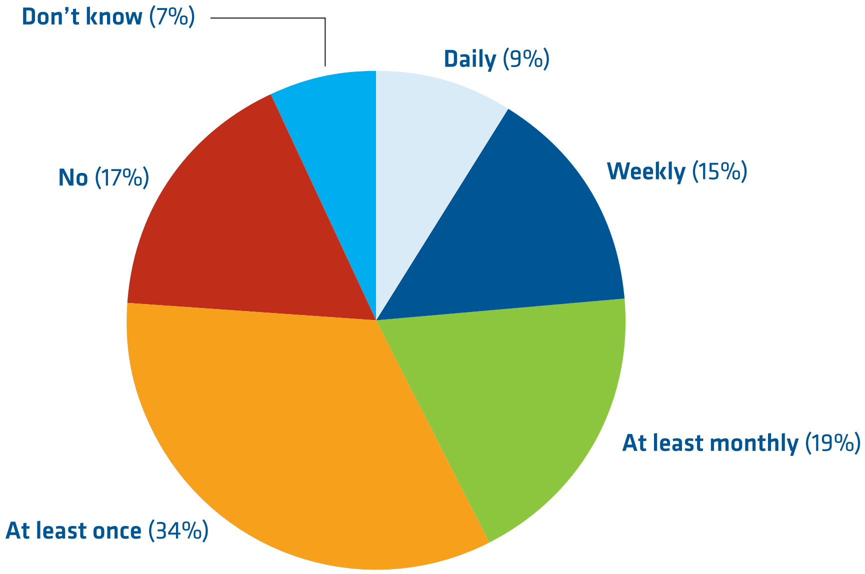
### Fig. 1 : How has the frequency/sophistication of cyber attacks involving customer-facing digital platforms changed at your organisation in the last two years?



Since lockdowns began in 2020, *Computing* research has uncovered rises in organised criminal gangs, ransomware attacks, phishing schemes, opportunistic hacks, social engineering, and incidents that prey on people's fears or medical needs, such as spoof NHS messages that seek people's personal details.

Not only are these incidents increasing in number, but they are also becoming more sophisticated and insidious, according to nearly 70 percent of respondents to our latest survey. In many cases, they target the organisation's customer-facing digital platforms – the front door of the enterprise.

## Fig. 2 : Has your organisation experienced cyber security attacks on its customer-facing digital platforms in the past 12 months?



Nine percent of respondents report daily attacks on those systems, 15 percent weekly incidents, and 19 percent monthly, while a further one-third have experienced at least one attack on customer systems since 2020.

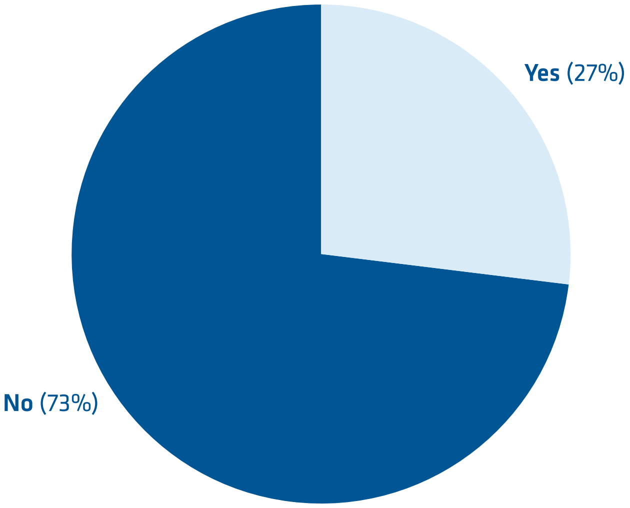
This puts any unprepared organisation's reputation in jeopardy, because a security failure could compromise customers' personal data, privacy, and/or their trust in its core brand values.

Trust can be expensively won over years of loyalty, and yet lost overnight. Reputational damage has a 'long tail' in these socially connected times: high-profile security failures and data losses are often talked about for years afterwards, inextricably linking brands with poor data protection.

Customers may be reluctant to do business with organisations in future if they know that personal data has been stolen from them – especially if those customers have had to change their own login details as a result, possibly across dozens of different sites and platforms.

Our research found that security fears are far from groundless or media scaremongering: over one-quarter of respondents (27 percent) report that their customer-facing digital platforms have been compromised by a cyberattack. That's a lot of successful incursions if you consider that there are roughly six million companies operating in the UK.

### Fig. 3 : Have your customer-facing digital platforms ever been successfully compromised by a cyber-attack?

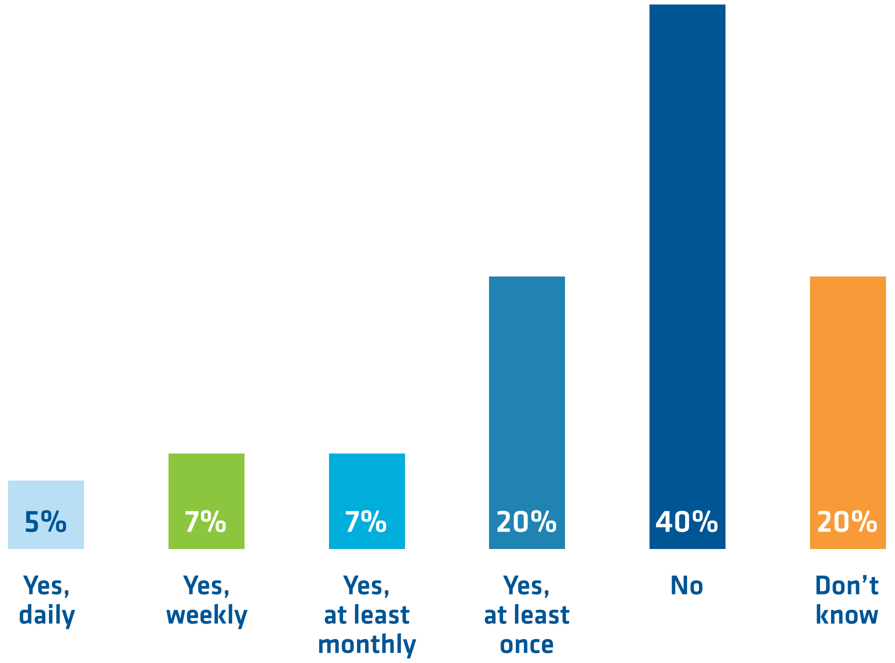


# Once more unto the breach

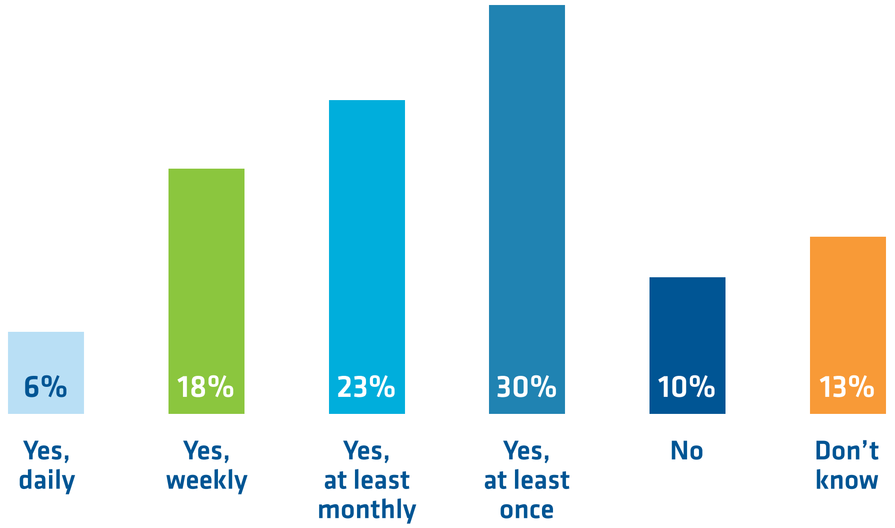
There is a good chance that the breach figures are even higher than that, judging by IT leaders' answers to follow-on questions in our survey. For example, nearly 40 percent of respondents say that their customer-facing systems have been accessed by someone falsely posing as a customer in the past 12 months – either daily, weekly, or monthly. Meanwhile, over three-quarters report that customers have been targeted by phishing/social engineering attacks since the crisis began – in many cases as often as weekly or monthly.

In some cases, of course, attacks may be coincidental: major brand names or platforms are often targeted indiscriminately at scale, on the off chance that random customers will fall for an email- or text-based scam. But those customers may still associate incidents with the brand itself. In other cases, the user, or groups of users, might be being tracked and targeted directly.

## Fig. 4 : Have your customer-facing digital platforms been accessed by someone falsely posing as a customer in the past 12 months?



## Fig. 5 : Have your customers been targeted with phishing/ social-engineering attacks in the past 12 months?



Whatever the reason for attacks, their impacts are certainly being felt by management. The ratcheting up of tension in (remote) boardrooms is evident in detailed responses to a range of other issues.

Our survey found that IT leaders are especially challenged by (in descending order):

1. Maintaining a secure online customer experience
2. Ensuring customer data is secure
3. Making sure it is also compliant with regulations – which may be in a state of flux, post-Brexit
4. Providing the best customer experience online
5. The ability to securely identify and authenticate users when they access services, often from a range of different devices
6. Achieving a measurable return on investment (ROI) from CIAM systems
7. Identifying the best method of multi-factor authentication
8. And scaling the CIAM solution across every channel – and the organisation as a whole

These interrelated issues are where the level of customer 'hoop jumping' becomes a critical consideration: organisations need to ensure that users are who they say they are and are authorised to use an account or service, but some customers dislike being forced into long, tortuous, or repetitive authentication procedures for some types of service.

They expect it from their bank, payment platform, or healthcare provider, for example, but they might be less tolerant of it from other platforms.

Get the balance wrong, and a transaction/relationship might tip from 'trusted' towards 'intrusive' or 'off-putting' in the customer's mind, particularly if users have to keep inputting the same details, clicking through endless screens, and authenticating themselves on a second device more than once.

That said, multi-factor authentication via customer number, passcode, text, app, or safety email address is a belt-and-braces approach that is increasingly popular and reduces the chance of unauthorised people accessing customer accounts.

However, some users might prefer to establish a bond of trust once, and not keep having to do it on every visit (unless they choose to clear their browser history and cookies because they are using a shared device). Listening to your customers and creating an appropriate experience for them is essential.

# Customer expectations

Of course, in the real world these perceived 'hoops' may be minor uses of a customer's time, compared to them taking a long journey into town, parking, and queueing in a branch, for example. But digital services have a tendency to make users demand instant gratification and simplicity. They want to 'see, click, and buy', with the transaction handled seamlessly in the background, and replicated across multiple channels.

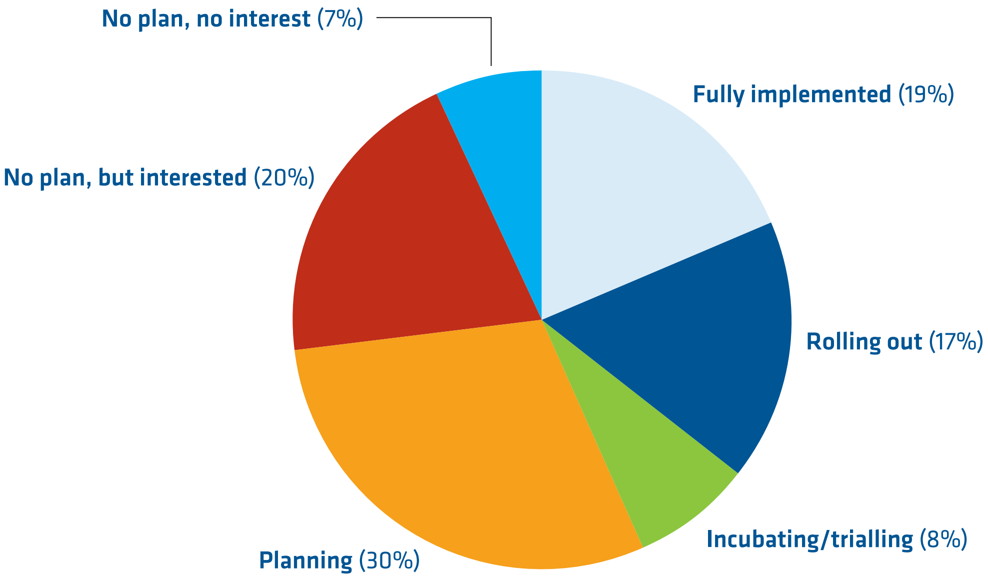
Users perceive time and value very differently online to on the high street, and perhaps rarely give the slowness or expense of real-world alternatives sufficient thought. That said, they are also voting with their fingers for whichever digital service is easiest and most pleasurable to use. Make it easy, seamless, and intuitive for them and they may reward you with their loyalty.

In this sense, customers are pushing all digital providers in the same direction of travel. The message is: 'Understand me, satisfy me, make me trust you, but don't get in my way'. Selfish behaviour, perhaps – the id meets the ID – but it is where we are in the 2020s.

But for the provider, security and authentication are essential, as is the ability to manage the customer relationship so that both sides are happy.

This is where advanced CIAM systems really shine and the best solutions should scale with user growth, control how customer data is shared, inject convenience and security at every stage of the customer journey, and, as a bonus, help you better understand your customers.

### Fig. 6 : To what extent has your organisation adopted an advanced customer identity and access management (CIAM) platform?

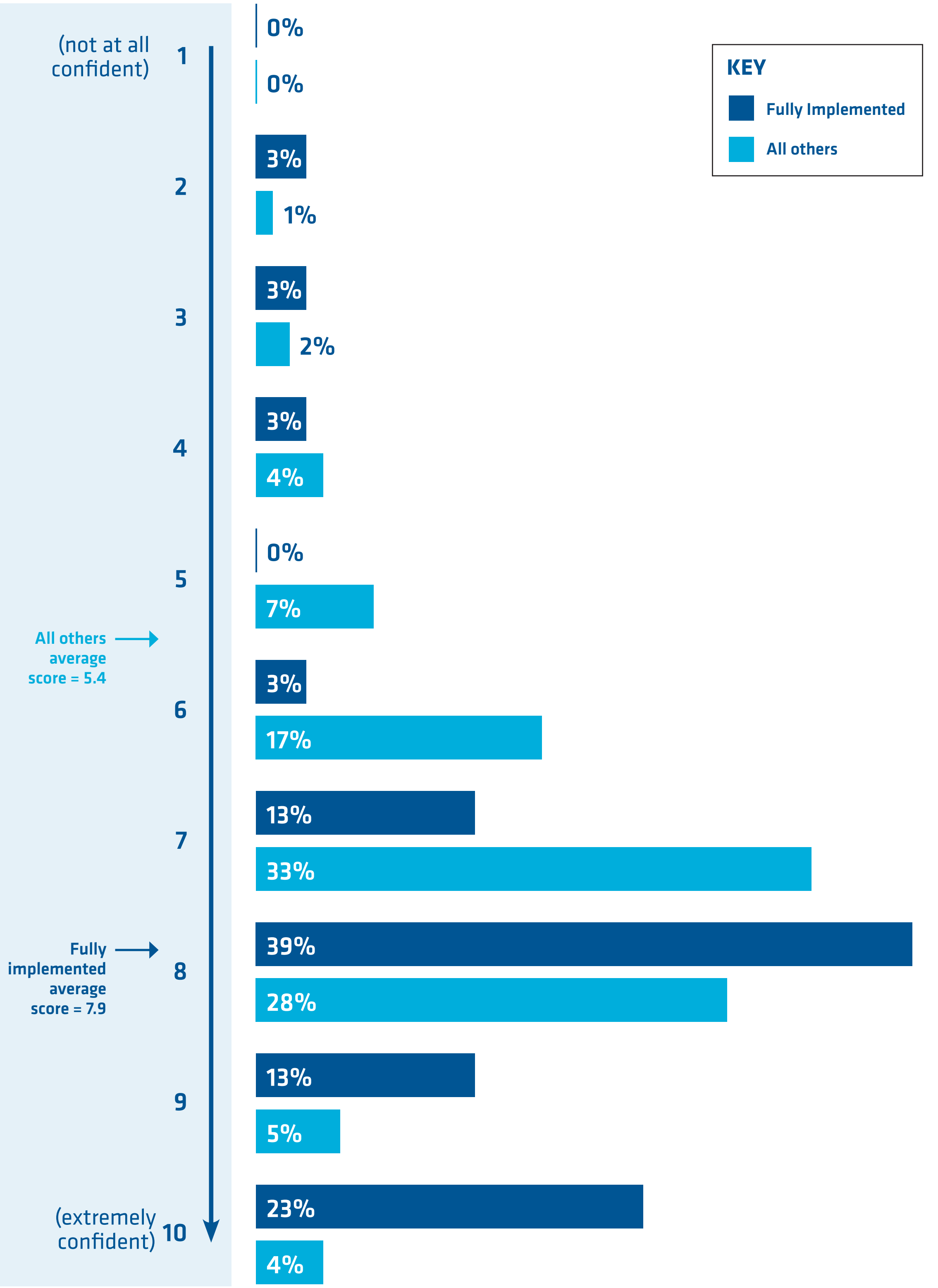


# So where are IT leaders on their CIAM journeys?

*Computing* found that a leading pack of one-fifth of respondents (19 percent) have already fully implemented advanced CIAM, with a further 17 percent actively rolling out the technology – that's a combined total of over one-third of organisations. A similar number are at an earlier stage in the process: eight percent are trialling and exploring their options, while another 30 percent are planning their move.

That leaves 20 percent with 'no plan but interested' and just over seven percent who have zero interest in the technology. Overall, therefore, IT leaders are split into three groups: leaders, followers, and also-rans.

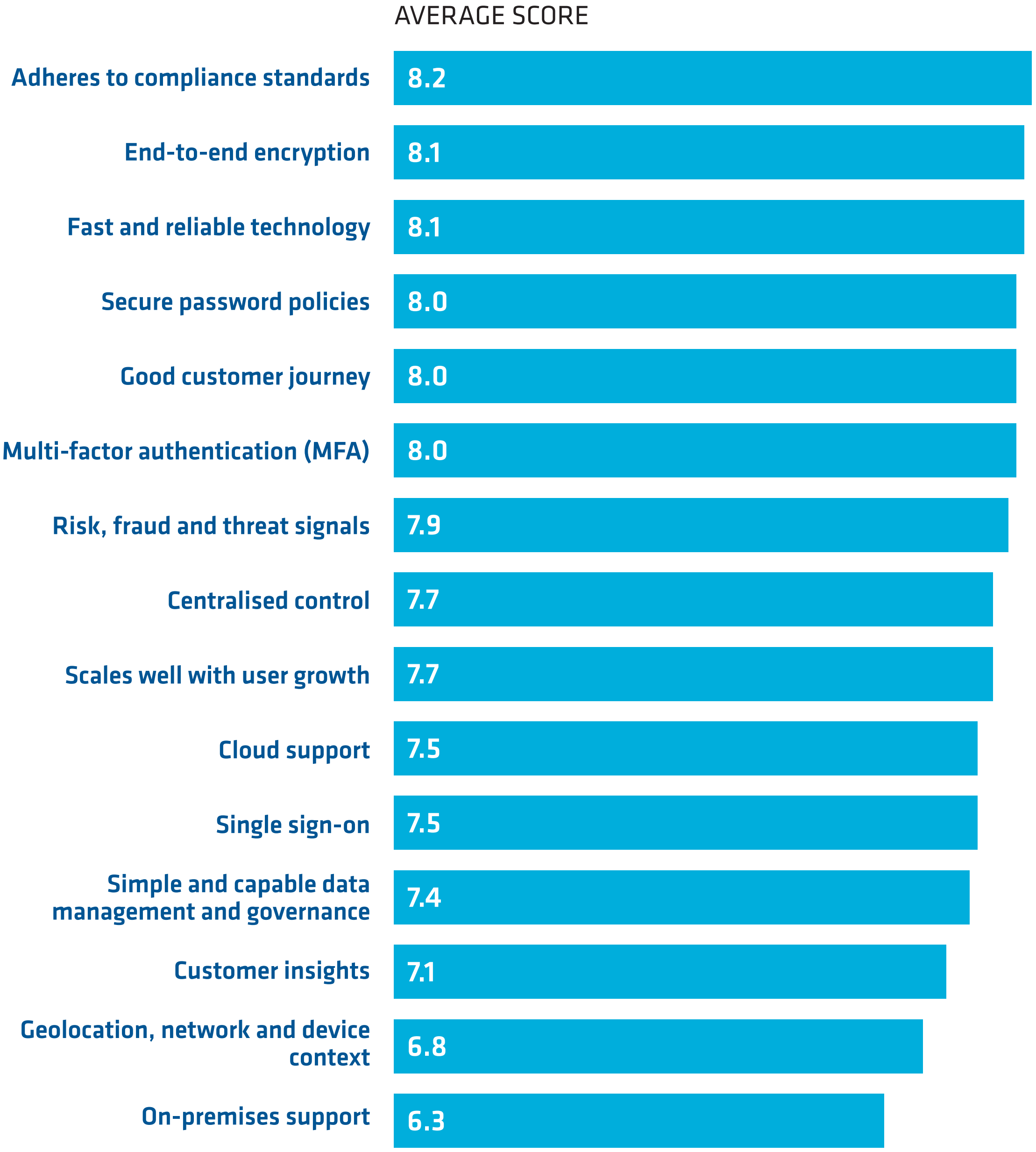
## Fig. 7 : On a scale of 1 (not at all confident) to 10 (extremely confident), how confident are you in the security of your processes for managing customer identities and access?



# Feeling confident?

So how confident are they in the security of their processes for managing customer identities and access? Asked to rate themselves on a scale from 1 (not at all confident) to 10 (very confident), the average score was 7.2. However, when this data is segmented between those that have fully implemented an advanced customer identity and access management (CIAM) platform and those that haven't, as in Fig. 7, it's clear that doing so significantly boosts confidence levels.

### Fig. 8 : On a scale of 1 (not at all important) to 10 (extremely important), how important are the following priorities/features to your organisation when it comes to choosing an identity and access management vendor?



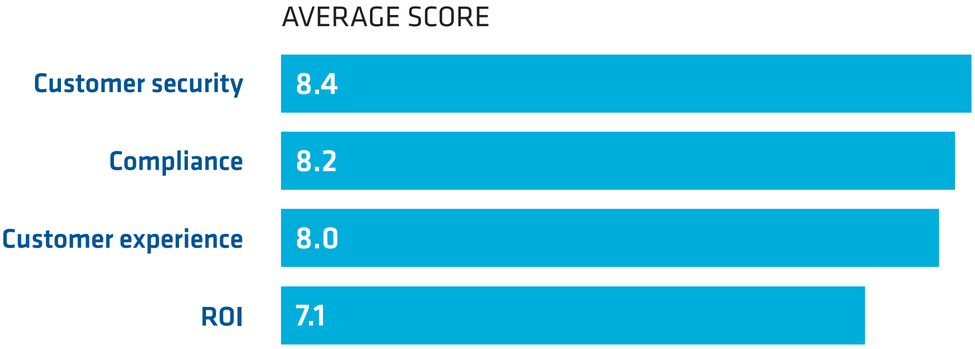
## Is convenience still king? Why good user experience and security must reign together in CIAM after the pandemic

As was seen in Fig. 8, asked what features are the most important in a CIAM offering, the most popular was 'adheres to compliance standards', with IT leaders rightly fearing the regulatory impact of any failure to manage customer data.

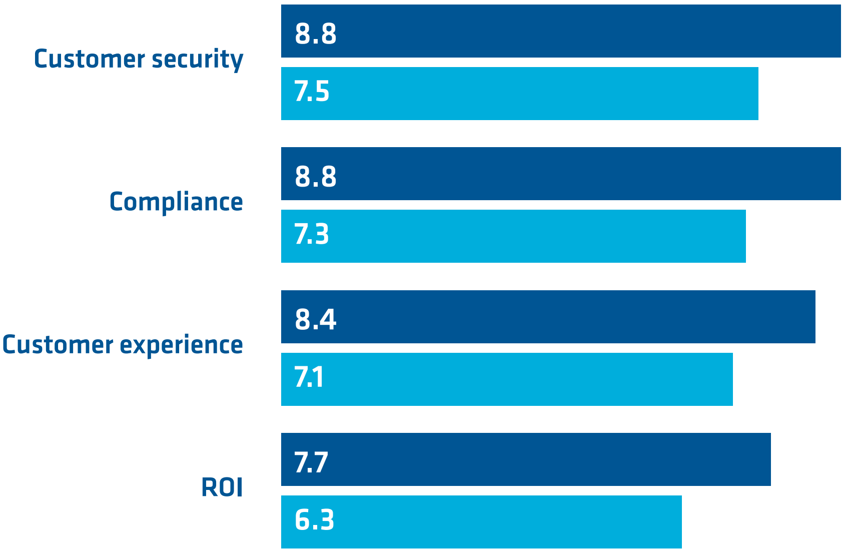
End-to-end encryption came second, despite that technology being frequently in the crosshairs of politicians, who perhaps fail to understand its critical importance to a range of business processes. Also highly favoured were 'fast and reliable technology'; 'secure password policies'; 'a good customer journey'; multifactor authentication; and risk, fraud, and threat signals.

According to Fig. 9, when it comes to CIAM decisions more broadly, compliance was seen as less important than customer security, though still ranked above a good customer experience, and a demonstrable return on investment from CIAM systems. All were seen as very important, however, in the UK's services-led economy.

### Fig. 9 : On a scale of 1 (completely irrelevant) to 10 (a top priority), to what extent does your organisation prioritise the following when making decisions relating to CIAM?



### Fig. 10 : On a scale of 1 (not at all successful) to 10 (completely successful), how successful have your organisation's CIAM solutions been in achieving the following?



As shown in Fig. 10, those organisations that have fully implemented an advanced CIAM solution have seen considerably greater success across the board, from security and compliance to customer experience. It's also worth highlighting that despite the likely greater cost of advanced CIAM solutions, they are performing better when it comes to ROI.

# Conclusion

We know that, with some exceptions, businesses have been forced online during the pandemic, and obliged to find new ways of reaching their customers. So, to what extent has the crisis also accelerated CIAM adoption?

In total, half of respondents said that Covid has either greatly or somewhat prioritised their use of the technology, with IT leaders pointing out customers' reliance on remote working, cloud systems, platforms, and apps, and the need for the organisation to match that desire with robust systems.

As they put it, "We can no longer rely on passwords alone to protect and identify customers online", and "Customer faith in our online security is vital to our success as a business." That's the key message, and the king of CIAM gets to wear the crown.

# About the sponsor, Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 6,500 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 9,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, T-Mobile, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers.

**For more information:**

**Visit:** www.okta.com

okta