itnews FOR AUSTRALIAN BUSINESS

Supported by transmit security

Securing Customer Identity Management in an Increasingly Challenging Era

Great customer experience is always important, but in today's on-demand digital world, customer identities and accounts are constantly targeted by evolving threats that demand advanced security and protection. Ensuring that great experience is secure is no longer a nice-to-have, but a necessity.

Customer identity and access management (CIAM) is the discipline of managing who can access your online services in a secure and easy way from the moment they touch your digital, or in-store, assets throughout the customer journey including account recovery.

Most organisations today have some form of customer-facing digital services, but many still lack the CIAM capabilities to keep up with the deceptive, automated security threats customers face. A solution that's purpose-built for customers should be able to protect accounts without hurting the customer experience. This requires accuracy that only an intelligent, context-aware solution can provide.

New insights into the emergence of CIAM

To understand how organisations will secure access to their applications with CIAM, iTnews and Transmit Security asked IT leaders about the importance of proper access management and how this is evolving with more options for access control. This includes evaluating risk predictors during the authentication and transaction flow coupled with real-time fraud behavioural monitoring throughout the user session.

To detect sophisticated fraud attacks, organisations now need a combination of real-time analysis of behavioural navigation, behavioural biometrics, device attributes and more. You must be able to correlate hundreds of signals to detect signs of account takeover fraud anywhere in the customer journey — from registration to account recovery and every step in between.

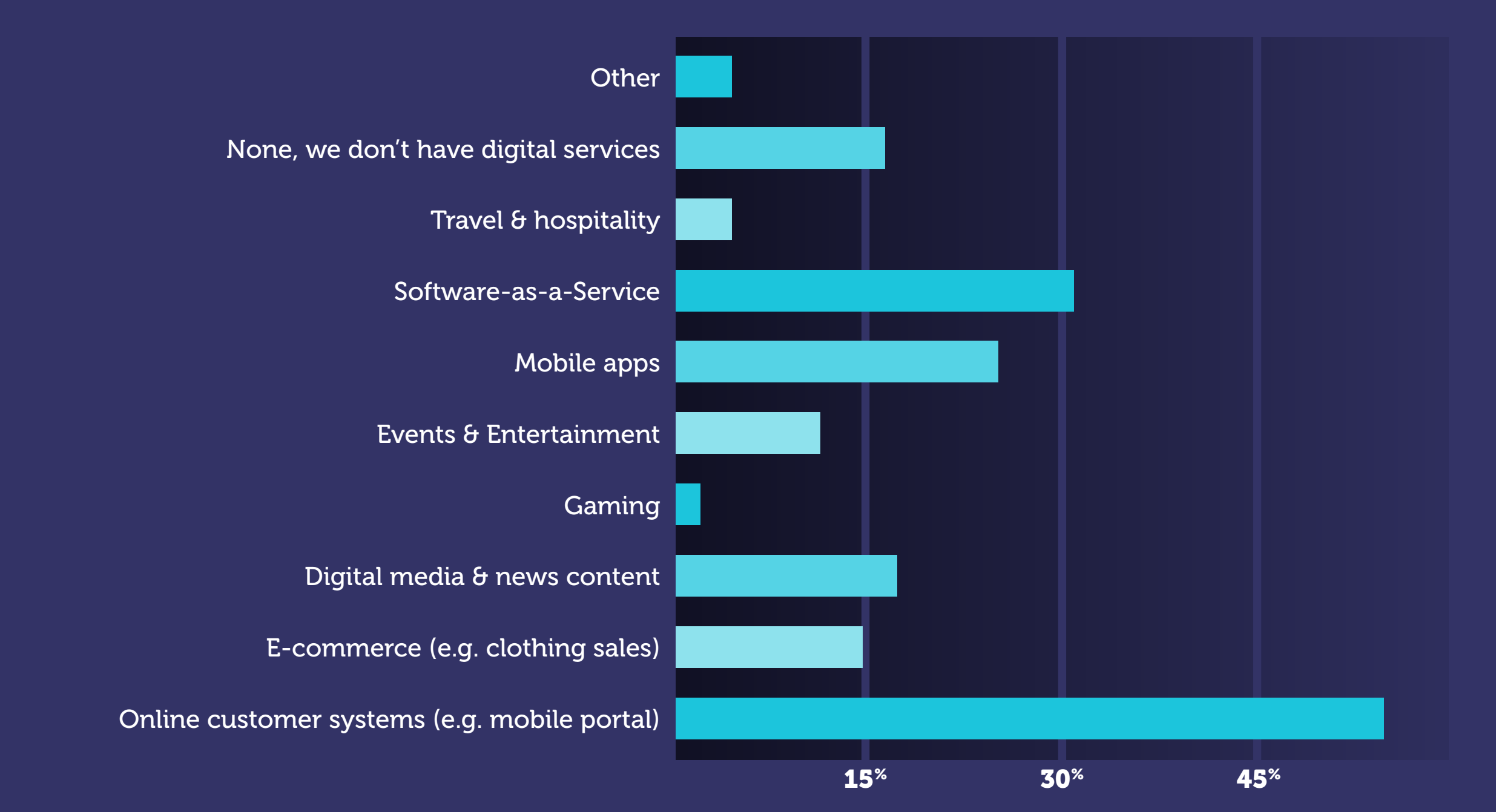
The research found a high 82 per cent of Australian organisations offer at least one type of customer account digital service, from mobile portals to e-commerce, indicating a high demand for CIAM.

However, a similarly high 75 per cent have no dedicated CIAM capability, which presents a large security and process improvement gap.

When it comes to CIAM, Australian organisations have many opportunities to improve how they secure and manage their customers' digital experiences and accounts.

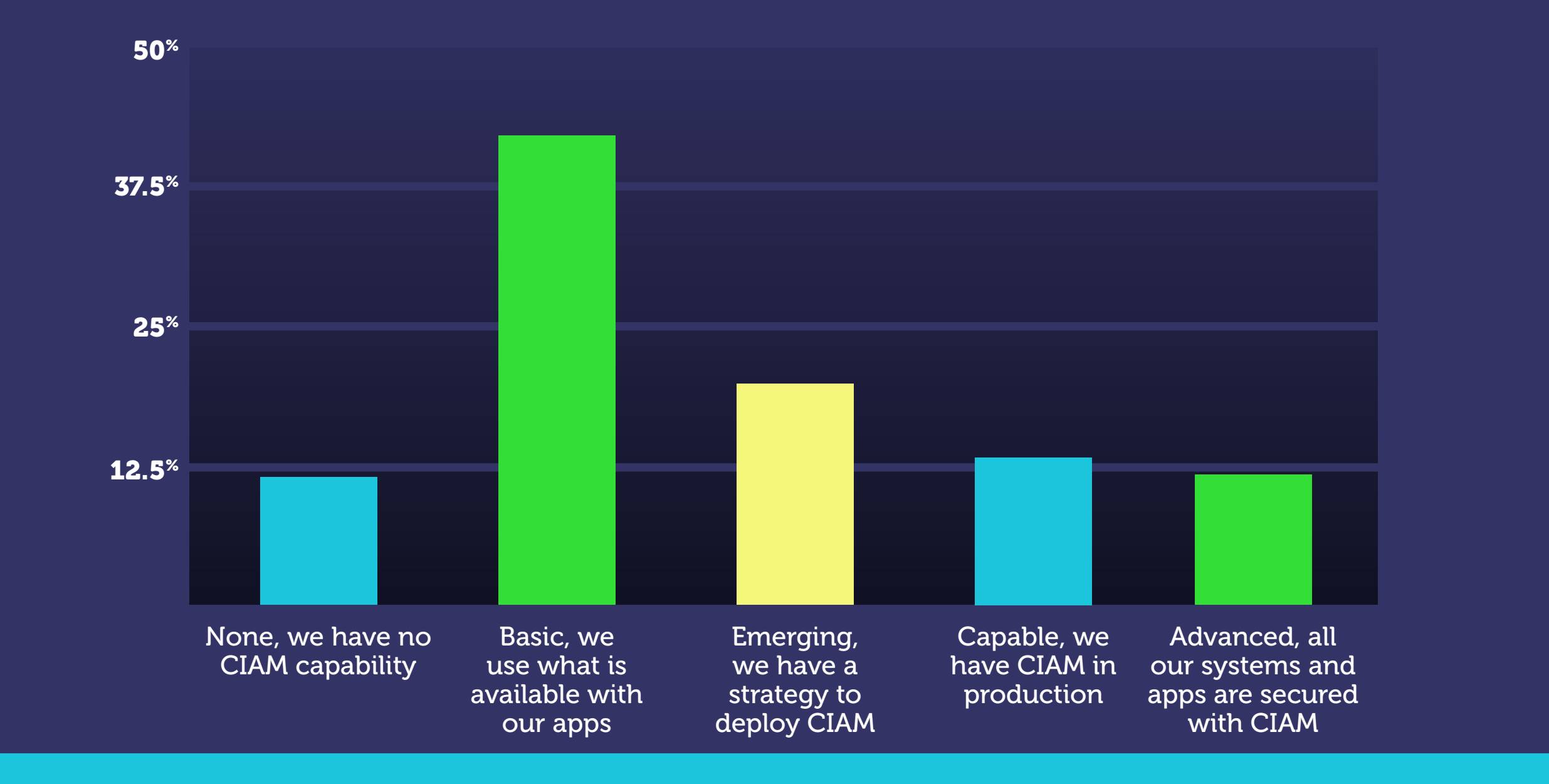
82% *of Australian organisations offer at least one type of online customer account digital service, from mobile portals to e-commerce, indicating a high demand for CIAM*

Please indicate what type of customer account digital services your organisation offers



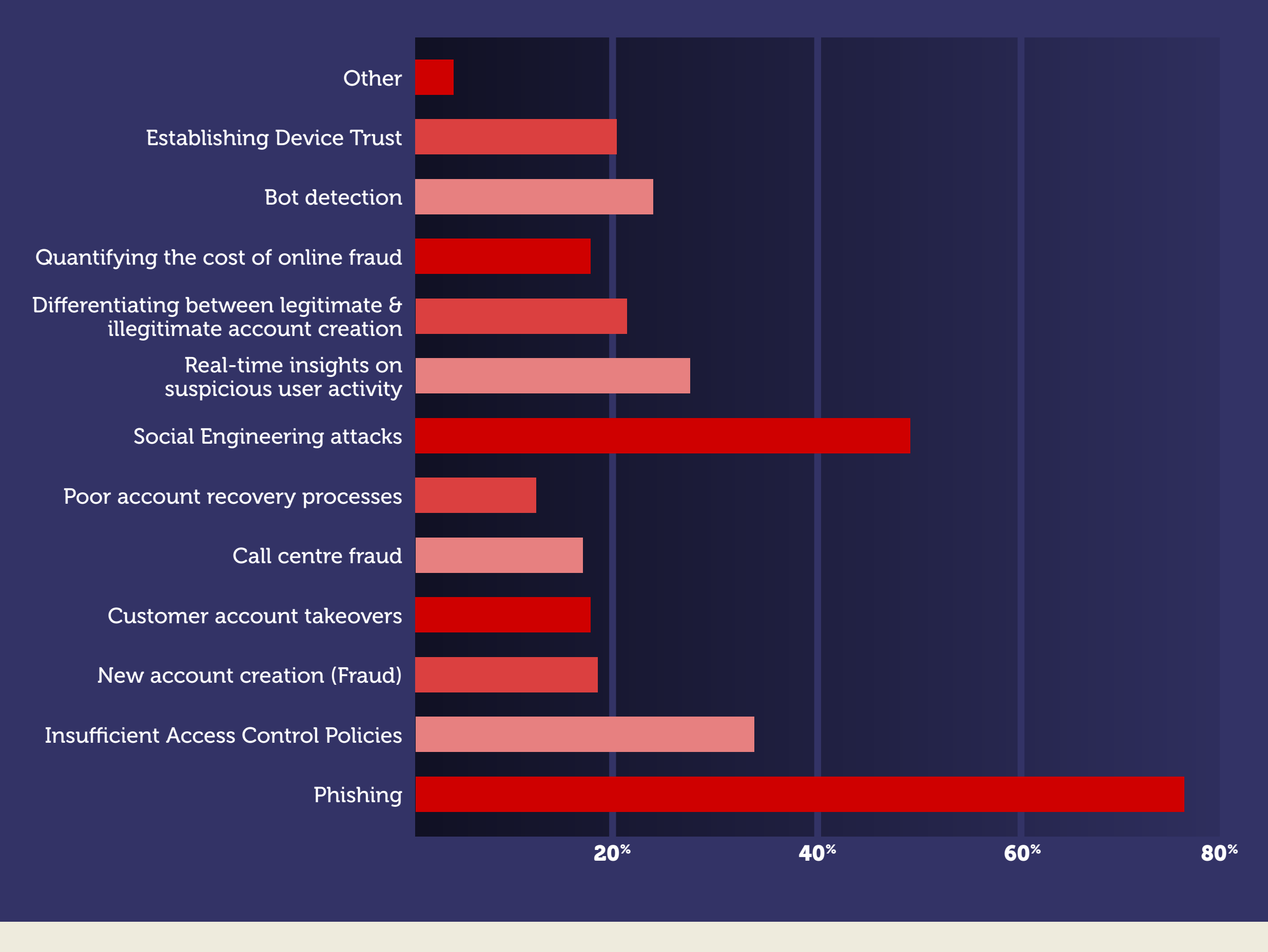
But **75%** *have no dedicated CIAM solution capability, creating a large security and process gap*

What is your organisation's maturity when it comes to customer identity and access management (CIAM)?



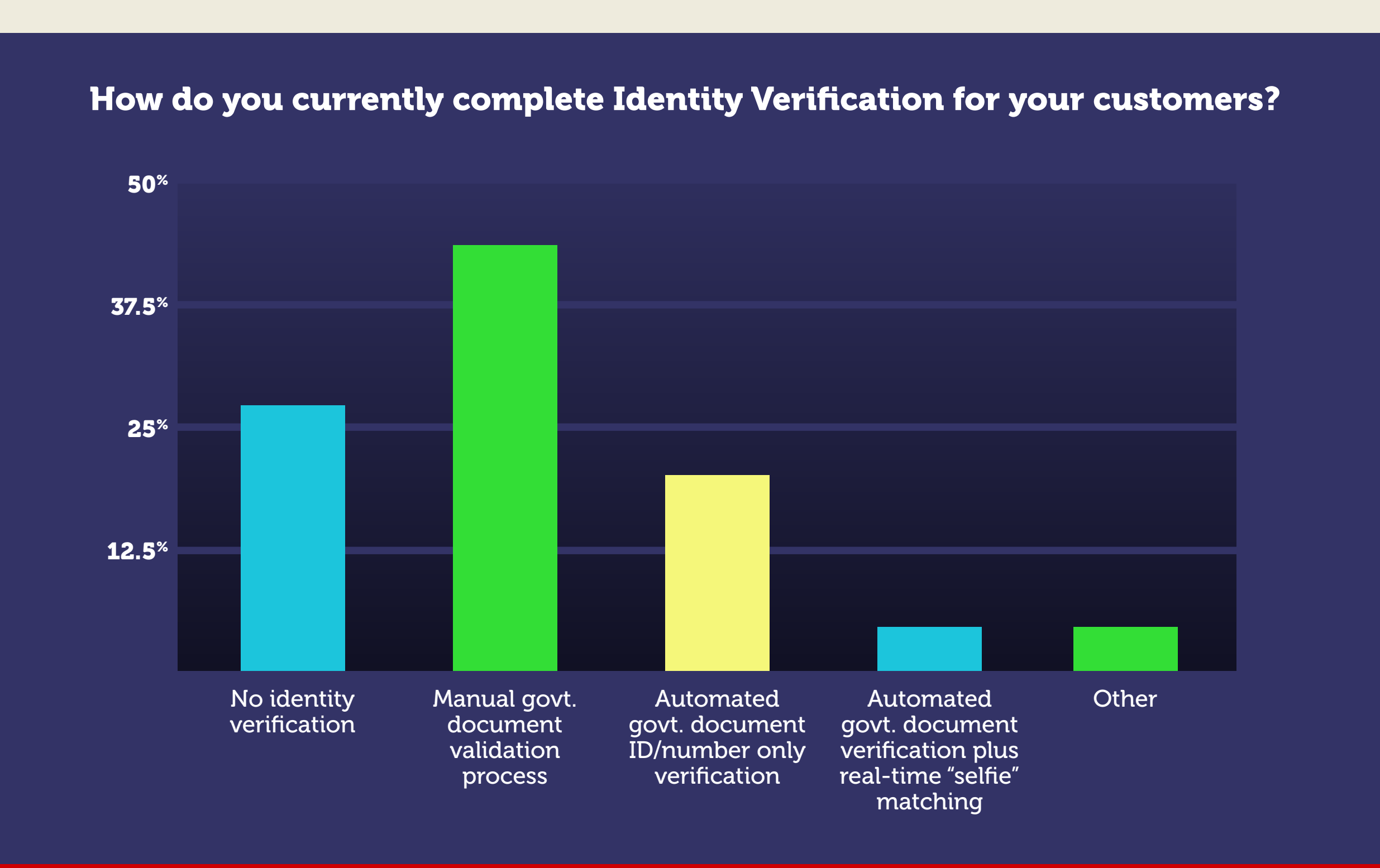
76% *of Australian organisations still see phishing as the biggest challenge around risk and fraud*

What are your biggest challenges today around risk and fraud?



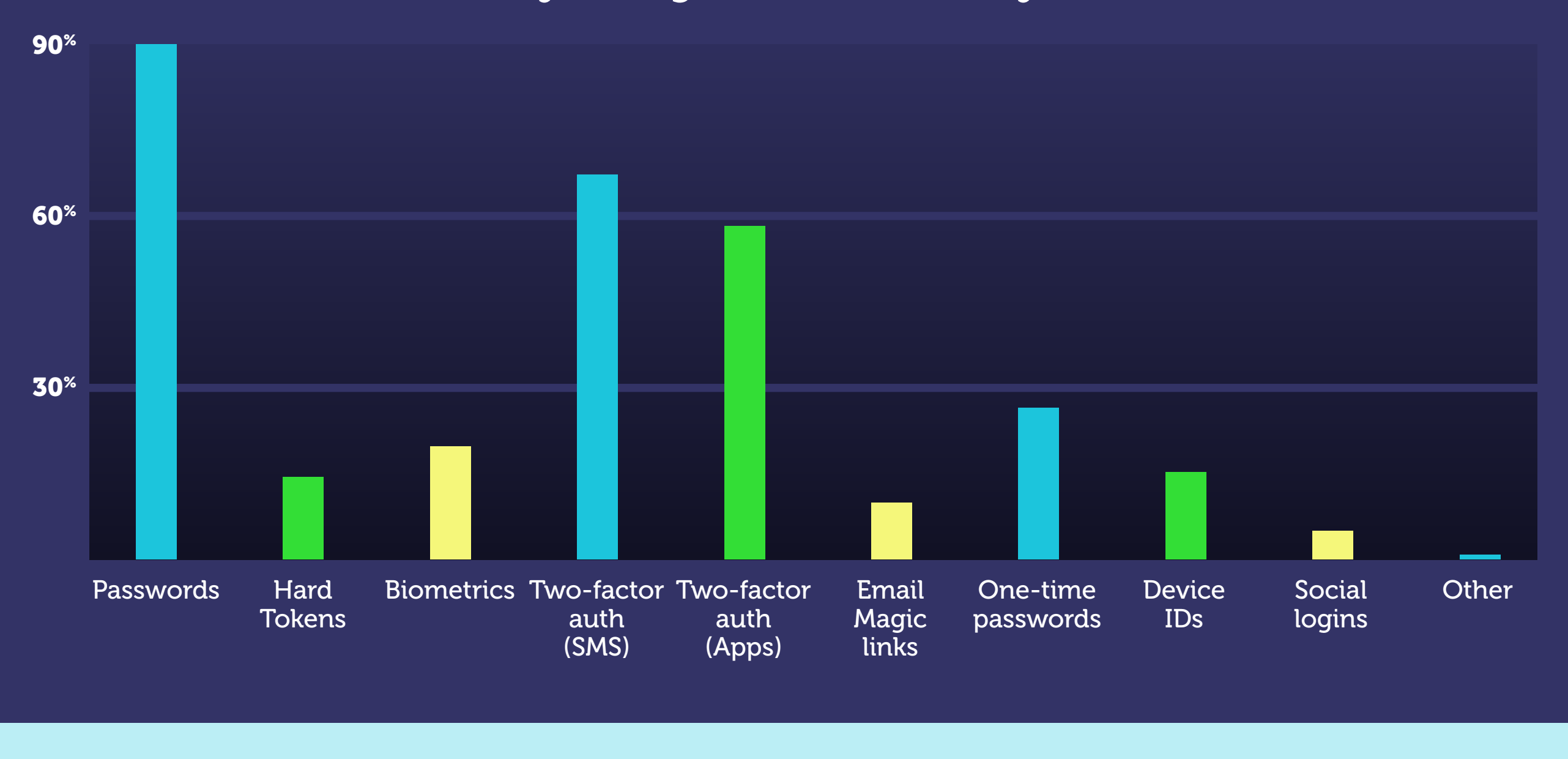
71% *of customer identity verification capability is still manual or missing entirely. Only* ***4%*** *have automated document verification plus real-time "selfie" matching*

How do you currently complete Identity Verification for your customers?



With passwords being the most common customer access control measure at **90%** *penetration*

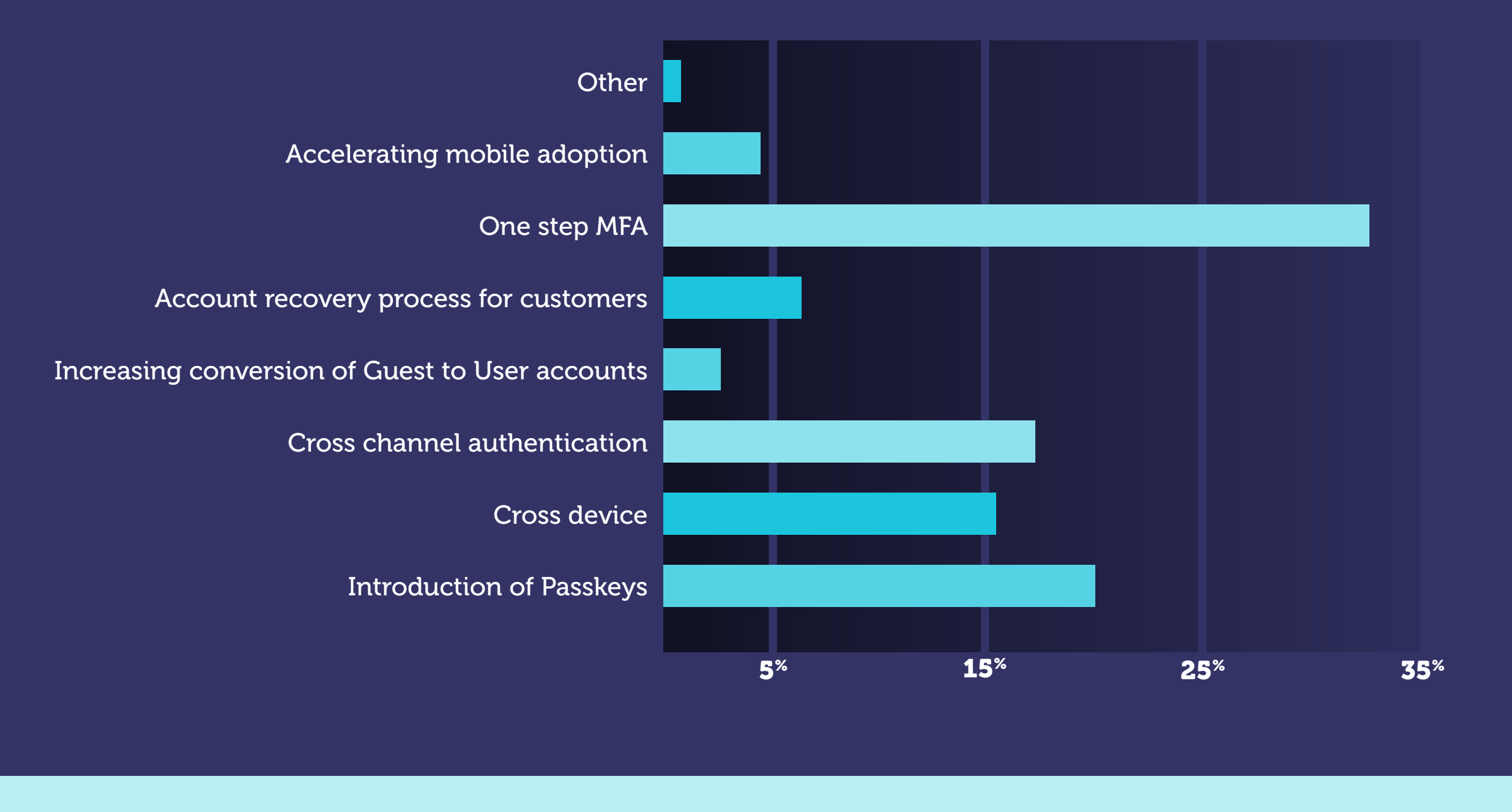
What customer access control measures does your organisation currently use?



1 in 3

IT leaders see ***one-step passwordless MFA*** *as the area of authentication of most relevance or interest*

Which of the following areas around Authentication are of most relevance or interest to your organisation

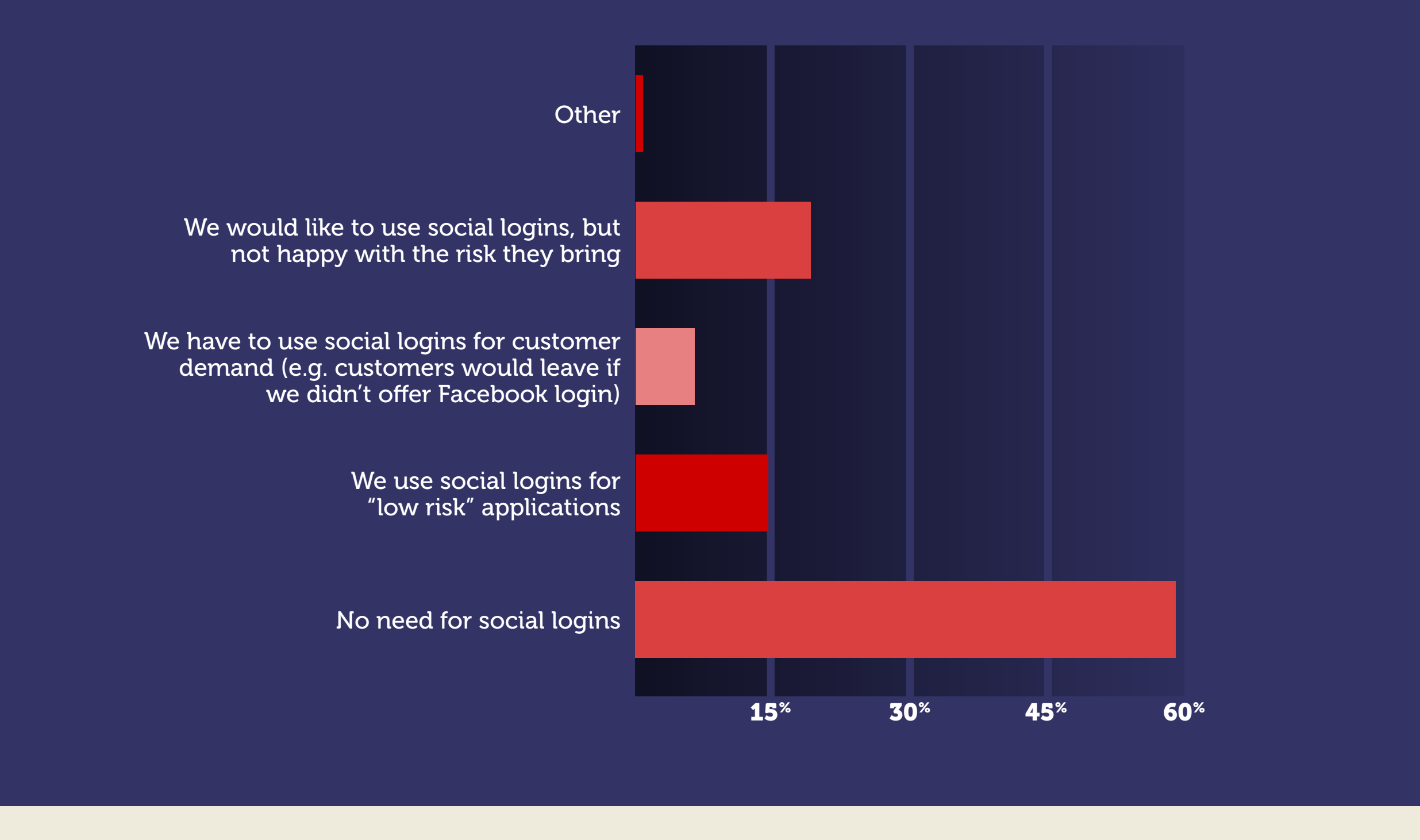


And **1 in 5**

are interested in ***passkeys****, an extension of FIDO authentication standards for passwordless MFA with a fingerprint or facial biometric plus a private key stored on the device (no database of password data to steal).*

59% *have no need for social logins and* ***19%*** *would like to use social logins, but are not happy with the risk they bring*

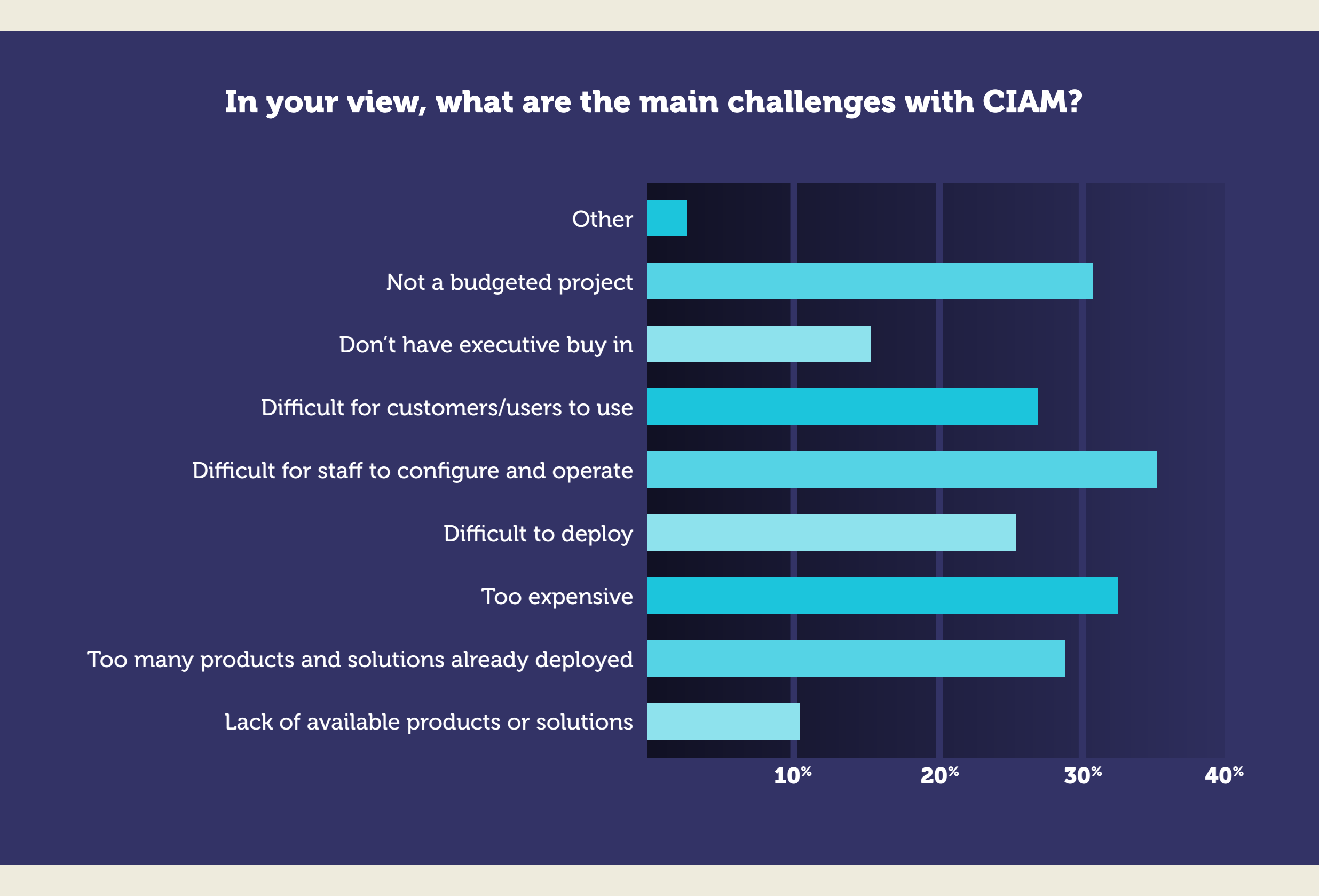
What is your organisation's view of social logins? Social logins allow customers to use the credentials from a social network (e.g. Facebook, Google) to access your digital services.



#1 challenge

IT managers see with CIAM is that it's difficult for staff to configure and operate, followed by expense

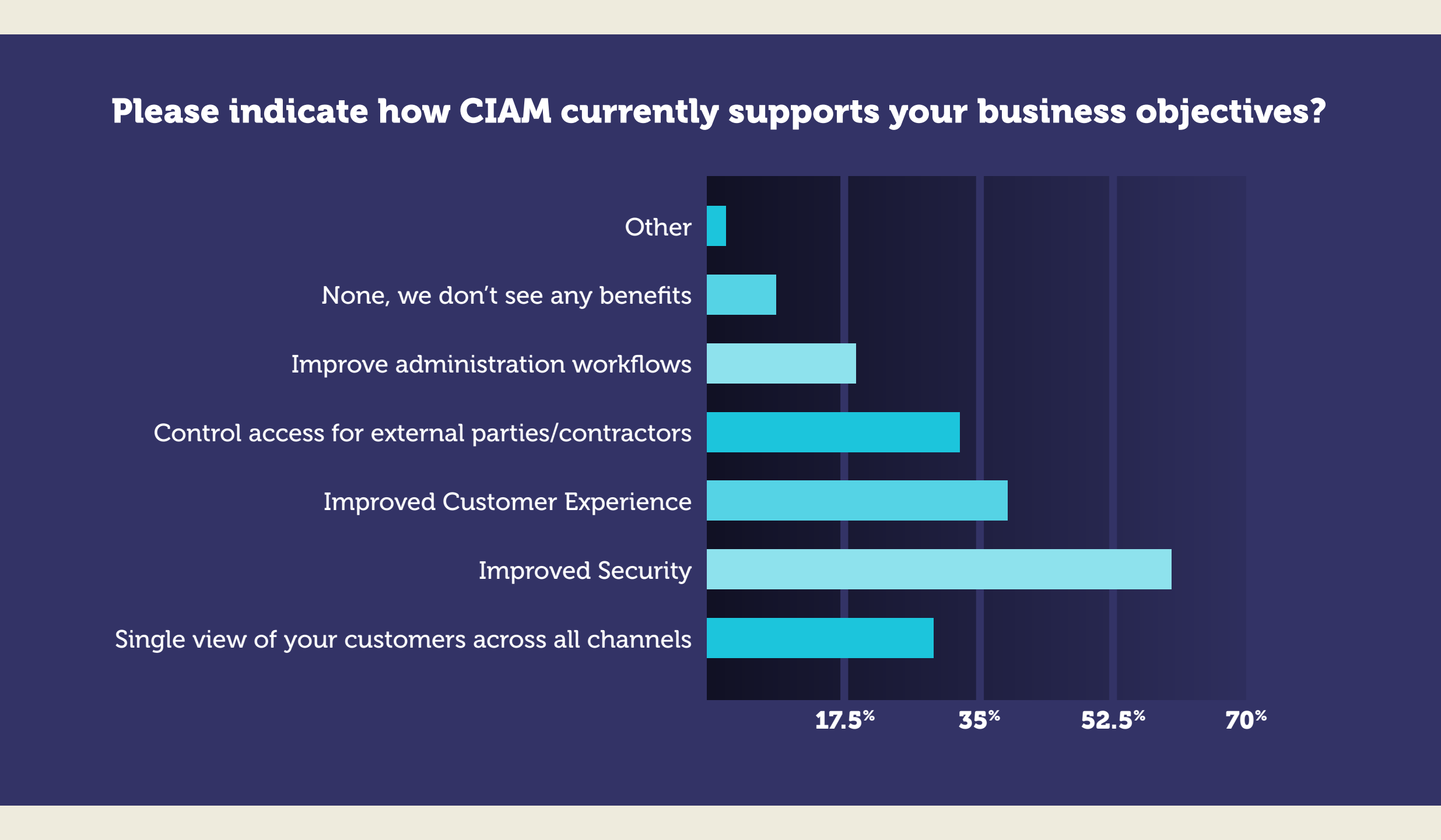
In your view, what are the main challenges with CIAM?



However, **90%+**

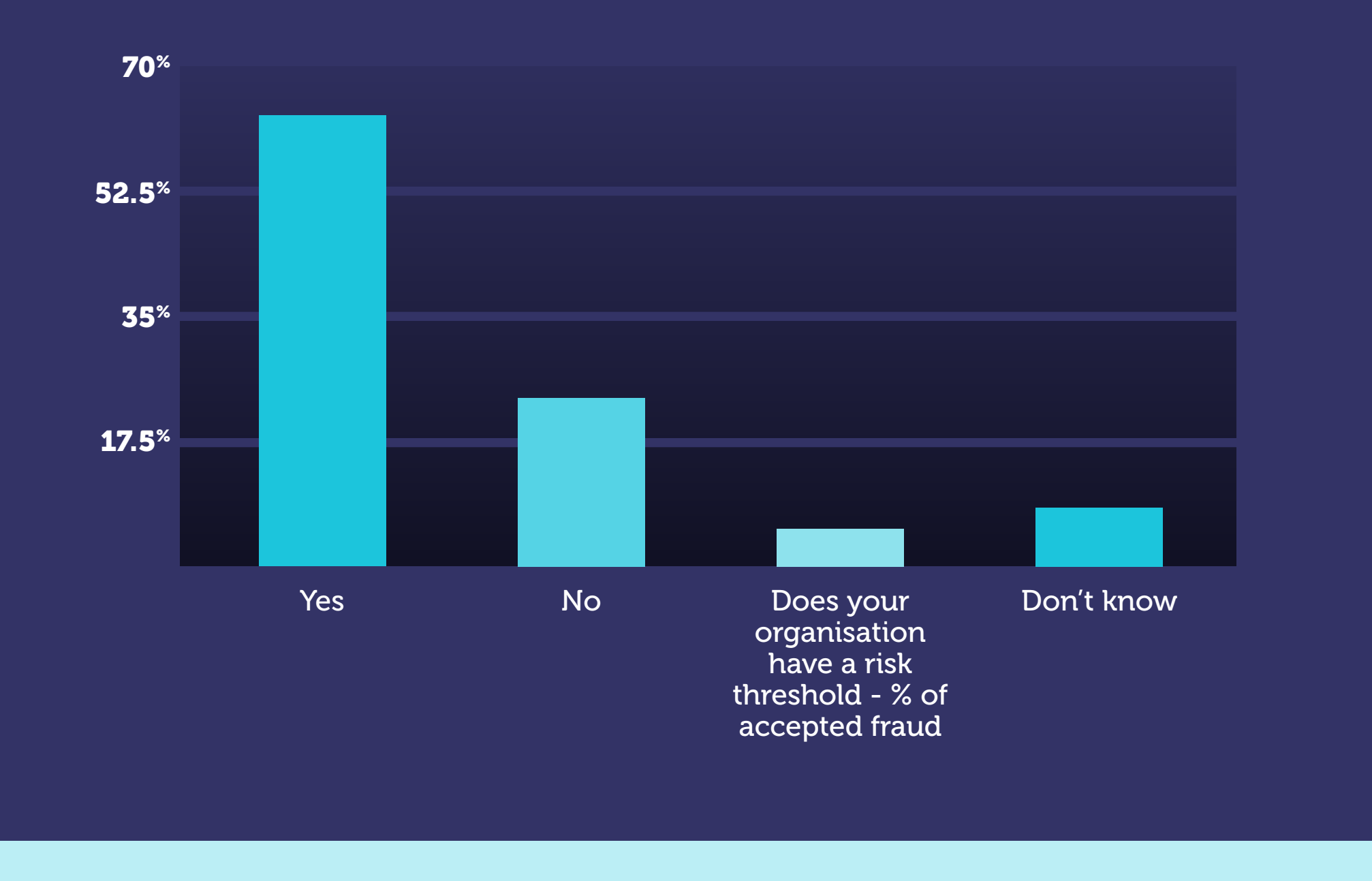
see benefits in how CIAM aligns with their supports business objectives, including improved security and customer experience

Please indicate how CIAM currently supports your business objectives?



And recent high-profile data breaches have made **63%** *of IT leaders more aware of the need for CIAM*

Have recent high-profile data breaches made your organisation more aware of the need for CIAM?



2 in 3

IT leaders prefer a ***cloud service or MSP delivery model*** *for CIAM solutions*

About the survey

This survey was conducted in November 2022 by iTnews on behalf of Transmit Security and attracted 110 respondents: 26.36% were IT managers or IT directors, 14.55% were IT professionals, including developers, analysts and engineers, and the rest included people in sales and marketing roles, CEOs, CFOs, GMs or MDs, those in analysis, consulting or education roles or similar, in addition to people in other roles. Looking at the size of their organisations, 26.36% worked for employers that have more than 2,500 staff members, 19.09% were at organisations with less than 10 people, while 17.27% worked for companies that employ 10-49 people.