The Role of Customer Identity Management in a Digital-First World

Authors:

Shweta Baidya
Linus Lai

IDC

Sponsored by

okta
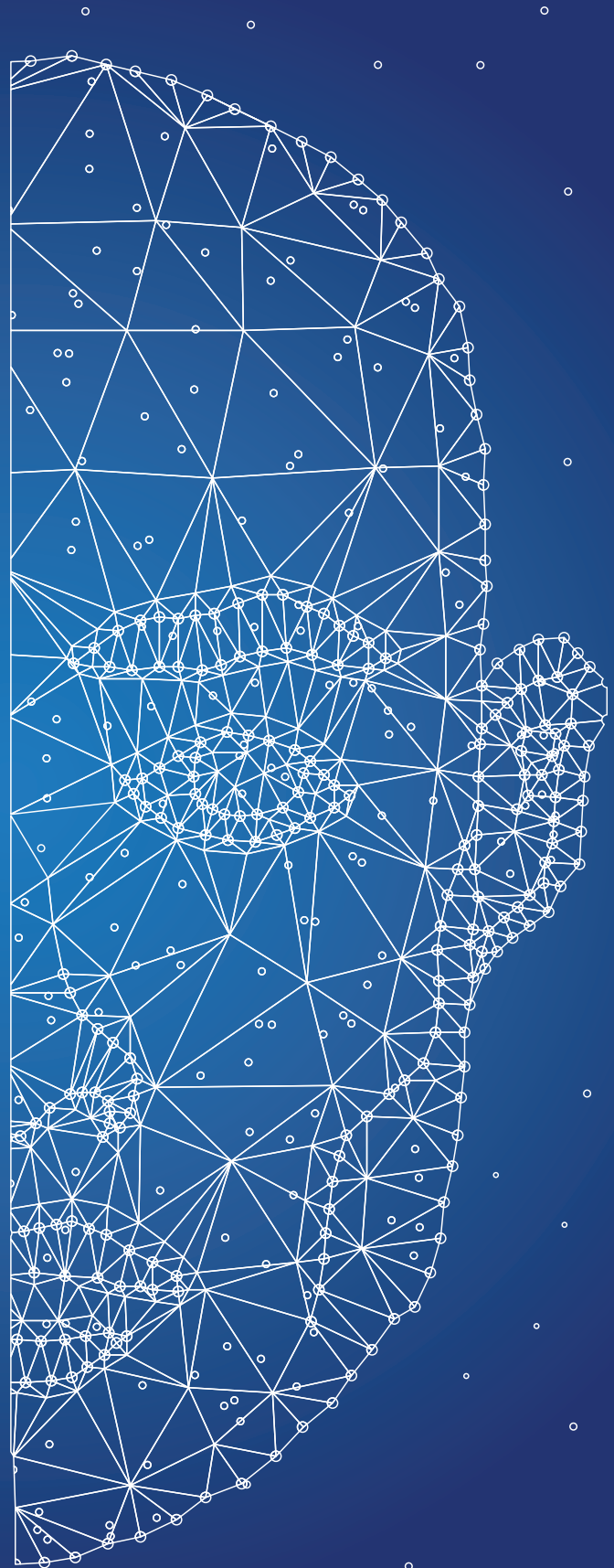
IDC opinion

In a digital-first world, customer requirements and expectations are rapidly evolving. CEOs are now fast progressing their digital transformation towards a digital-first (DF) strategy with the goal of creating and delivering digital value through contextualisation and real-time insights at scale. This requires a complete mindset shift and leaders need to think of creating new products/solutions that are suitable for digital platforms first.

A digital-first experience is not only about providing immersive and personalised experiences for customers, but also about building customer trust through data privacy and security. Securing the digital identities of customers has become a key priority and necessity for organisations of all sizes.

This IDC White Paper explores the dynamics of managing customer identity and access in a digital world and how digital-first organisations fare against their peers. IDC's 2022 survey of 750 Asia/Pacific organisations revealed the following findings:

- The pandemic has either accelerated or highlighted the need for digital-first strategies for 72% of Asia/Pacific organisations, with another 21% having already anticipated the need for such strategies prior to COVID-19. These digital-first leaders are more likely to prioritise customer satisfaction, agility, and innovation beyond traditional metrics such as revenues, and are more likely to report an improvement versus their peers in key customer metrics.

- Malicious cyberattacks, multiple channel access, customer privacy, scale, and compliance were cited as top challenges in managing customer identity and access.

- Among digital-first leaders, 56% have already deployed customer identity access management (CIAM), with another 32% planning deployment in the next 12–24 months. However, despite increasing adoption of CIAM, a majority of the enterprises are yet to reach the maturity stage in their CIAM implementations.

- 34% of digital-first leaders versus only 14% of digital-first followers have adopted an advanced approach towards CIAM, wherein customer identities are managed via a CIAM platform with full integration to enable 360-degree customer views and deliver a highly personalised experience. They are also more likely to invest in advanced CIAM capabilities such as passwordless access, consumer-focused seamless authentication, setting context-based access policies, among others.

- Digital-first leaders with advanced CIAM maturity organisations are 1.5x more likely to overperform their expectations in key metrics, such as new customer acquisition, customer loyalty, digital talent attraction and retention, and time to market for new products and services.

72% of Asia/Pacific organisations realise the need for digital-first strategies

Top challenges

56% of digital-first leaders have deployed CIAM

34% of digital-first leaders have advanced CIAM approach
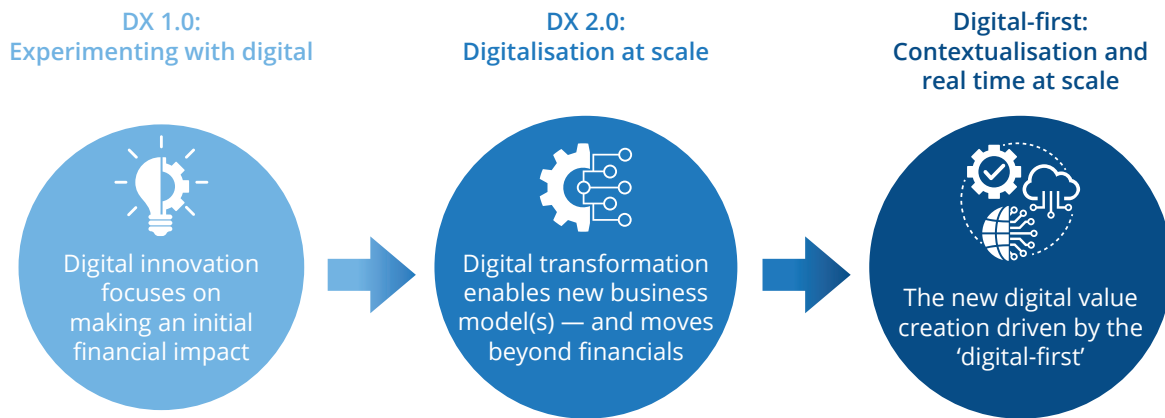
1.5x more likely to outperform

From digital transformation (DX) to digital-first

IDC predicts that by 2022, more than half the global economy will be based on or influenced by digital technologies. To compete and succeed in this increasingly digital world, enterprises must adopt a digital-first strategy. Digital-first takes digital transformation to a different level and redefines the definition of value. Digital-first is not a technology or a business model, but can be defined as an organisation's aspiration and characteristic as a digital business. To be digital-first, an organisation must constantly ask: "Is there a digital-based capability/enhancement that could improve our lives and desired outcomes?"

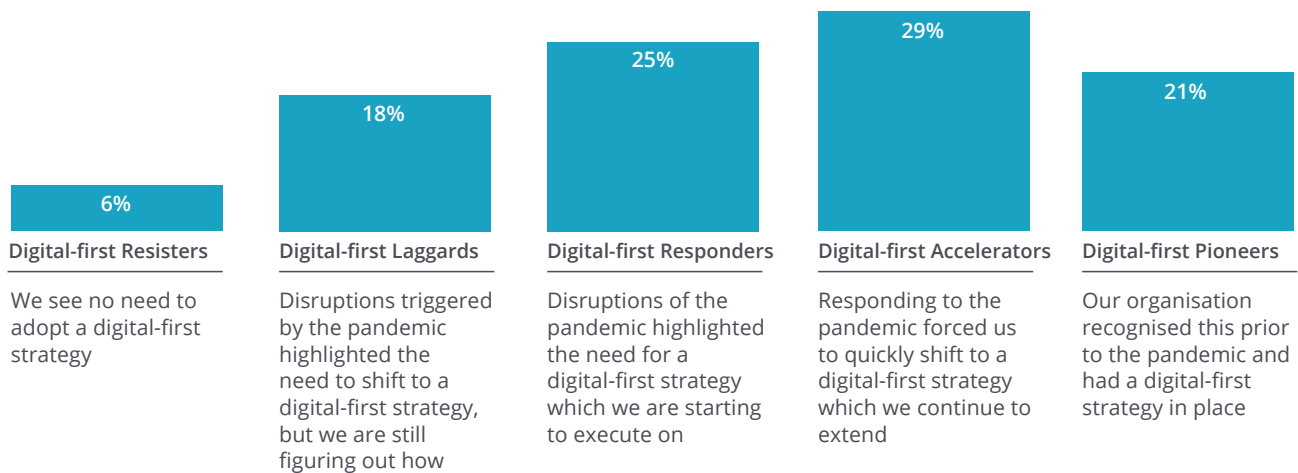Figure 1: **From DX to digital-first: Redefining value creation**

DX 1.0:
Experimenting with digital

Digital innovation focuses on making an initial financial impact

DX 2.0:
Digitalisation at scale

Digital transformation enables new business model(s) — and moves beyond financials

Digital-first:
Contextualisation and real time at scale

The new digital value creation driven by the 'digital-first'

Source: IDC, 2022

The pandemic has either accelerated or highlighted the need for digital-first strategies for 72% of Asia/Pacific organisations, with another 21% having the foresight to anticipate the need for such strategies prior to the pandemic. The digital-first leaders (Accelerators and Pioneers) have an enterprisewide strategy and long-term investment in place for going digital. **To put it simply, the digital and overall business strategy is one of the same for these organisations.**

Figure 2: **Digital-first strategy adoption**

Q. Which of the following best describes your organisation?

Digital-first Resisters	Digital-first Laggards	Digital-first Responders	Digital-first Accelerators	Digital-first Pioneers
6%	18%	25%	29%	21%
We see no need to adopt a digital-first strategy	Disruptions triggered by the pandemic highlighted the need to shift to a digital-first strategy, but we are still figuring out how	Disruptions of the pandemic highlighted the need for a digital-first strategy which we are starting to execute on	Responding to the pandemic forced us to quickly shift to a digital-first strategy which we continue to extend	Our organisation recognised this prior to the pandemic and had a digital-first strategy in place

Source: IDC's Asia/Pacific Customer Identity & Access Management Survey, sponsored by Okta, April 2022, N=750

Customer experiences at the forefront of digital-first strategy

Digital-first leaders are more likely to prioritise customer satisfaction, business agility, and innovation beyond traditional metrics such as revenues. Such priorities naturally put customer experience (CX) at the forefront of a digital-first strategy. The focus on CX has driven digital-first organisations to re-evaluate their customer engagement strategies in order to create seamless multichannel and real-time experiences.

Digital-first organisations are more likely to have broad awareness and enterprisewide strategies and budgets to provide a personalised CX. They have managed to align their overall business goals with customer experience management that eventually leads to better outcomes. They are investing in customer experience management technologies and processes to build a trusted, secure, and cohesive environment for customers to engage with. Contrast this with the rest of the market that often lacks a clear enterprisewide vision or road map for CX, resulting in disparate solutions and approaches.

While the pandemic has undoubtedly driven up customer online traffic and support volume for most organisations, not surprisingly, digital-first organisations are more likely to report an improvement versus their peers in customer satisfaction and retention, beyond traffic and support volume.
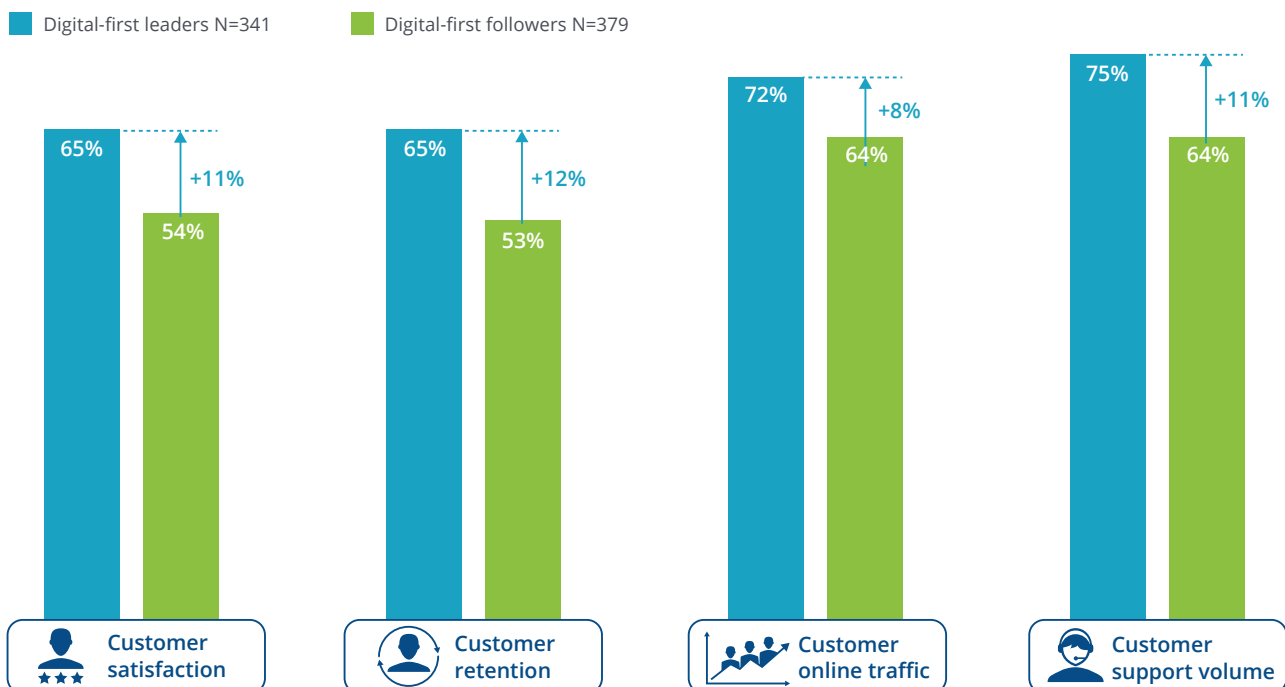
> " By 2023, enterprises that excel at empathy and safety at scale will outperform those that don't by 40%. "
>
> — *IDC's Worldwide Future of Customer and Consumer 2022 Predictions – Asia/Pacific (Excluding Japan)*

Figure 3: **Performance across customer metrics**

Q. Which of the following best describes your organisation's performance on these customer-related metrics in the last 12 months?

% of organisations that reported performance increase in metric

■ Digital-first leaders N=341   ■ Digital-first followers N=379

	Customer satisfaction	Customer retention	Customer online traffic	Customer support volume
Digital-first leaders	65%	65%	72%	75%
Digital-first followers	54%	53%	64%	64%
	+11%	+12%	+8%	+11%

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=720

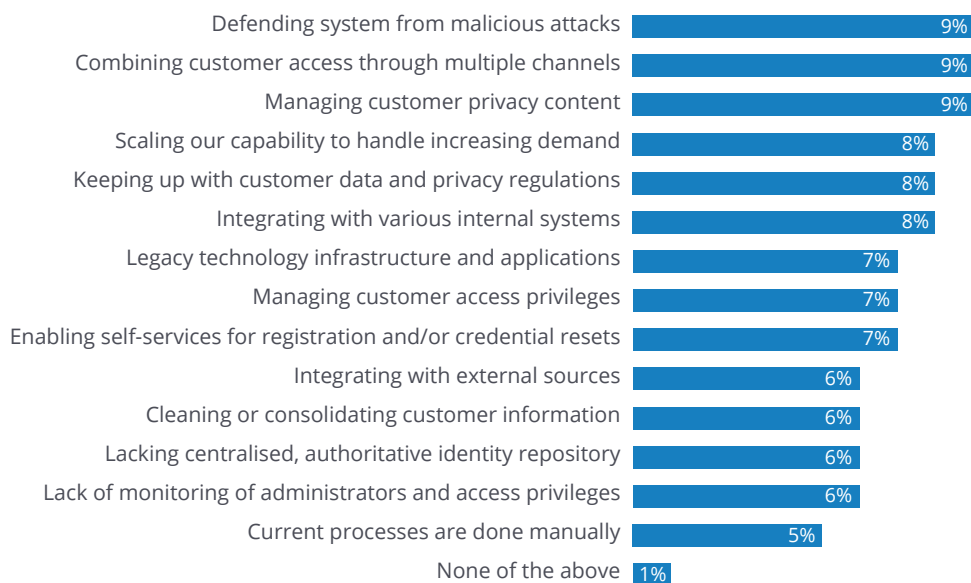# Securing identity in a digital-first world

Challenges with identity

The pandemic has forced enterprises to embrace a digital-first strategy. These digital-first organisations are re-imagining ways to improve efficiencies, productivity, and experiences across the whole ecosystem involving vendors, partners, customers, and suppliers. However, these transformations brought up a number of challenges, especially around customer identity verification and access security. Malicious cyberattacks, multiple channel access, customer privacy, scale, and compliance were cited as top challenges in managing customer identity and access.

Figure 4: **Challenges in managing identities**

Q. What are your organisation's top 3 challenges in managing your identity and access?

Challenge	Percentage
Defending system from malicious attacks	9%
Combining customer access through multiple channels	9%
Managing customer privacy content	9%
Scaling our capability to handle increasing demand	8%
Keeping up with customer data and privacy regulations	8%
Integrating with various internal systems	8%
Legacy technology infrastructure and applications	7%
Managing customer access privileges	7%
Enabling self-services for registration and/or credential resets	7%
Integrating with external sources	6%
Cleaning or consolidating customer information	6%
Lacking centralised, authoritative identity repository	6%
Lack of monitoring of administrators and access privileges	6%
Current processes are done manually	5%
None of the above	1%

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=750

Securing the digital identities of customers as well as the larger ecosystem players is considered table stakes in ensuring the success of a digital-first strategy. Hence, investments in customer/consumer identity and access management technologies have become a necessity in order to enable a secure and personalised digital experience. CIAM solutions provide organisations with better visibility to threats across systems, allowing for better defence from malicious cyberattacks. Furthermore, complying with customer data and privacy regulations such as the Privacy Act 1988 (Australia), Personal Data (Privacy) Ordinance (Hong Kong), Personal Data Protection Bill (India), the Act on the Protection of Personal Information (Japan), General Data Protection Regulation (Europe), is becoming more complex. CIAM solutions provide the ability to handle the complexity that comes with increasing customer identity volume and governance across multiple channels.

Attaining greater CIAM maturity

Digital-first leaders understand the importance of CIAM and are taking stringent identity and data protection measures to nurture digital trust and offer a better customer experience. This was evident in our research which showed that 78% of digital-first leaders surveyed agree that CIAM is among their top investment priorities in their organisations, versus only 60% of digital-first followers. Without a complete and thorough control mechanism, identity and data confidentiality can be compromised and might have an adverse impact on a company's revenue and reputation in the long run.

As a result, there is a strong trend towards adopting CIAM technologies among digital-first leaders. Our survey showed that 56% of digital-first leaders have already deployed CIAM, with another 32% planning to deploy such technologies in the next 12–24 months. However, despite increasing adoption of CIAM, a majority of the enterprises have not yet reached the stage of maturity in their implementation. CIAM maturity entails evaluating and implementing the technology centrally across the organisation and not in silos or as a piecemeal solution. Organisations that have an enterprisewide strategy to implement CIAM platforms for seamless and smooth customer journeys are considered to be in the advanced stage of maturity. Our research shows different stages of CIAM adoption for digital-first leaders and digital-first followers (Figure 5). It is not surprising that digital first organisations are ahead in their CIAM maturity.

Figure 5: **CIAM maturity in Asia/Pacific**

Q. Which of the following best describes customer identity and access management in your organisation?

Digital-first followers N=365   Digital-first leaders N=380

58% 32% — Disparate
28% 34% — Enabled
14% 34% — Advanced
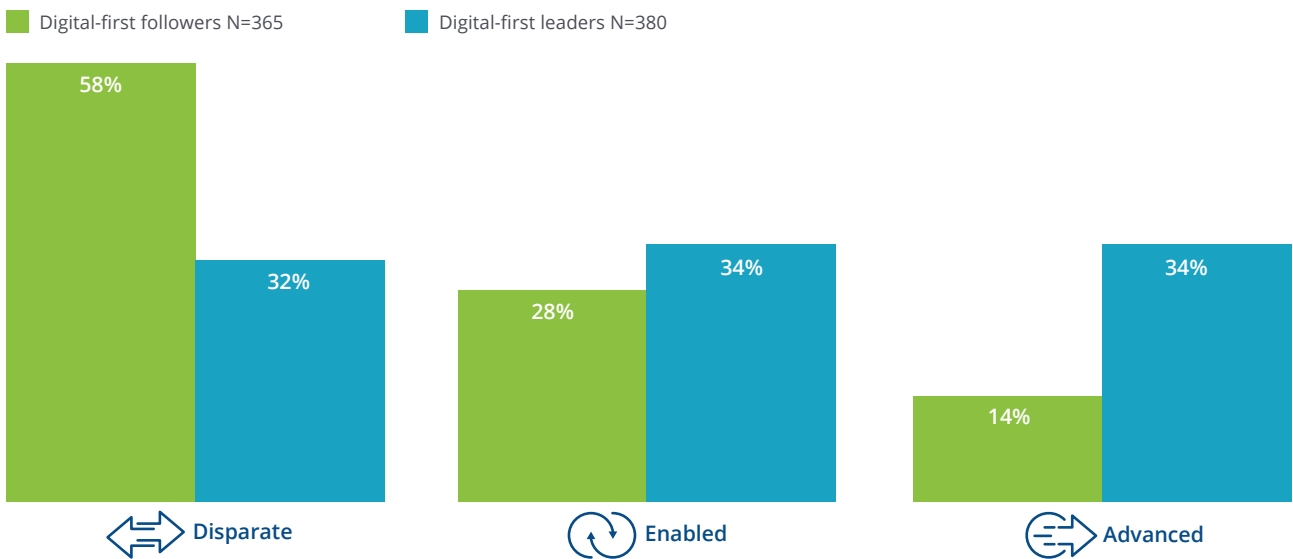
Stage 1 — Disparate

Disparate technologies and processes without a guiding enterprise-level strategy. Identities are single-purpose and do not extend across channels.

Varying CIAM technologies used across channels, but many are connected through single sign-on.

Stage 2 — Enabled

CIAM is governed centrally, enabling seamless customer journeys through digital enrolment and authentication. Data protection and privacy compliance requirements are met across all jurisdictions.

Stage 3 — Advanced

Customer identities are managed via a common CIAM platform with full integration to all onboarding, fraud, anti-money laundering (AML), and customer relationship management (CRM) applications to create a complete 360-degree customer view.

CIAM platforms enable delivery of highly personalised experiences. Open APIs enable connections to external identity schemes and drive new business models and revenue streams.

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=745

58% of digital-first followers invested in disparate technologies and processes where identities are not managed or governed centrally. The focus is on point products rather than CIAM platforms. In this earlier stage, the customer identity verification process is arduous due to multiple registration/sign-in requirements, increasing the likelihood of customer dissatisfaction.

More than 1/3rd of digital-first leaders are at Stage 2 (enabled) and well-focused on their CIAM journey with investments being governed centrally, which helps in enabling seamless customer experiences. The

organisations at the Enabled stage have done the groundwork to ensure data protection and privacy are in compliance across multiple jurisdictions.

The difference is clearly visible as organisations move towards the advanced stage of maturity. Compared to 34% of digital-first leaders, only 14% of digital-first followers have an advanced approach towards CIAM, wherein customer identities are managed via a CIAM platform with full integration to enable a 360-degree customer view and deliver a highly personalised experience, thereby offering opportunities for new business models and revenue streams.

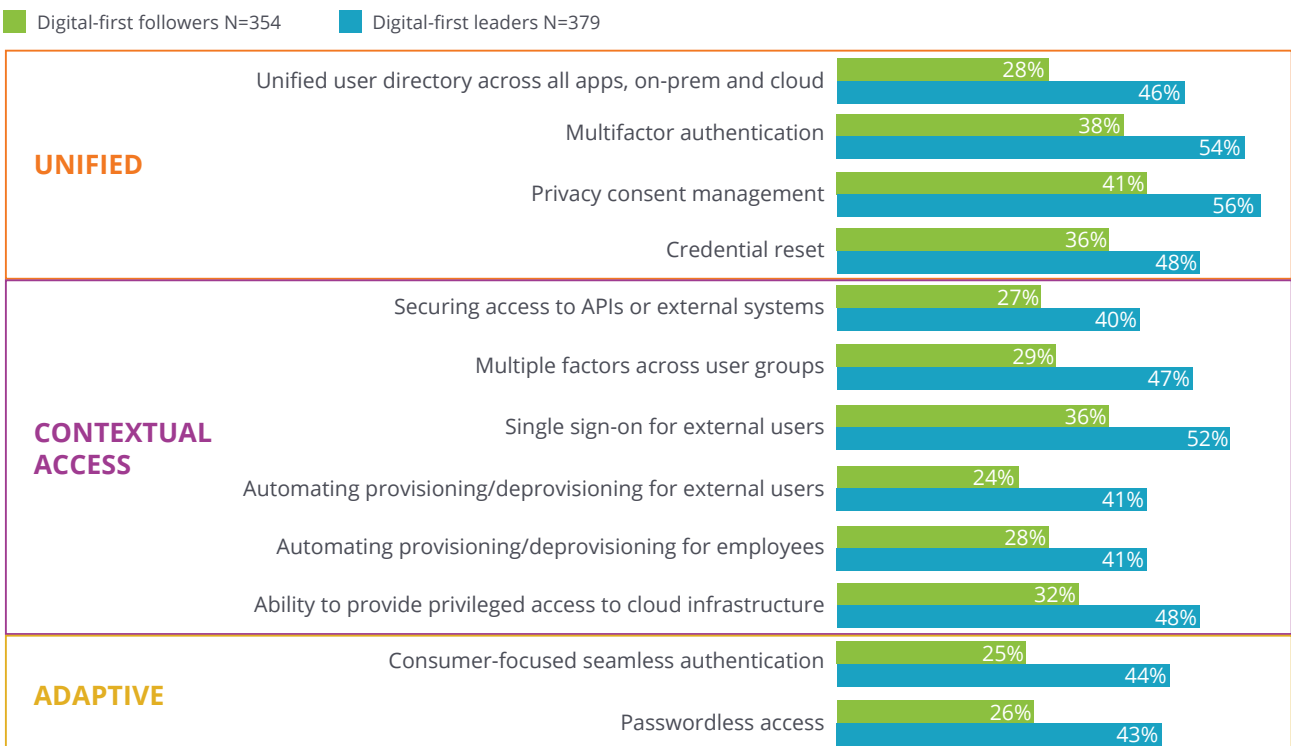## Investing in contextual and adaptive CIAM capabilities

Interestingly, most enterprise investments in identity and access management (IAM) have traditionally had an inward focus. The solutions focus on managing employees' identities and are not relatively adept in managing external customers' and partners' identities. The traditional IAM does not typically prioritise the user experience (UX), scalability, and flexibility needed to handle external stakeholder authentication processes.

While most organisations today realise the need for identity management solutions and have invested in

foundational capabilities such as multifactor authentication (MFA), single sign-on, and unified user directory, digital-first organisations are taking the leap further with investments in advanced CIAM capabilities such as passwordless access, consumer-focused seamless authentication, setting context-based access policies. As a result, digital-first organisations enjoy a stronger and more adaptive cybersecurity posture, better management of customer data, optimisation of long-term costs, and increased productivity.

Figure 6: **CIAM capabilities**

Q. Which of the following has your organisation deployed to manage customer identity and access within your organisation?

■ Digital-first followers N=354   ■ Digital-first leaders N=379

UNIFIED

Unified user directory across all apps, on-prem and cloud	28% / 46%
Multifactor authentication	38% / 54%
Privacy consent management	41% / 56%
Credential reset	36% / 48%

CONTEXTUAL ACCESS

Securing access to APIs or external systems	27% / 40%
Multiple factors across user groups	29% / 47%
Single sign-on for external users	36% / 52%
Automating provisioning/deprovisioning for external users	24% / 41%
Automating provisioning/deprovisioning for employees	28% / 41%
Ability to provide privileged access to cloud infrastructure	32% / 48%

ADAPTIVE

| Consumer-focused seamless authentication | 25% / 44% |
| Passwordless access | 26% / 43% |

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=733

CIAM investments resulting in tangible benefits

CIAM solutions yield a range of benefits such as operational efficiencies, improved security, and enhanced customer experience. Digital-first organisations saw a positive impact by simplifying or automating authentication processes and providing a uniform customer identity experience across all channels. Moreover, CIAM solutions also help digital-first organisations to be compliant. Compliance has been challenging for many enterprises dealing with customers with multiple digital identities, spread across geographies with different data protection and sovereignty regulations. CIAM solutions enable organisations to be compliant with respect to collecting, storing, and analysing the data of their customers without compromising on other aspects such as security, ease of access, flexibility to connect across different devices and touch points.

Figure 7: **Customer/consumer identity and access management benefits**

Q. What are the top 3 business benefits that your organisation has achieved (or is expecting to achieve) by investing in customer identity and access management solutions?

Benefit	%
Operational efficiency	22%
Improved security posture	19%
Enhanced customer experience	17%
Regulatory compliance	15%
Lower total cost of ownership	14%
Faster time to market	12%

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=750
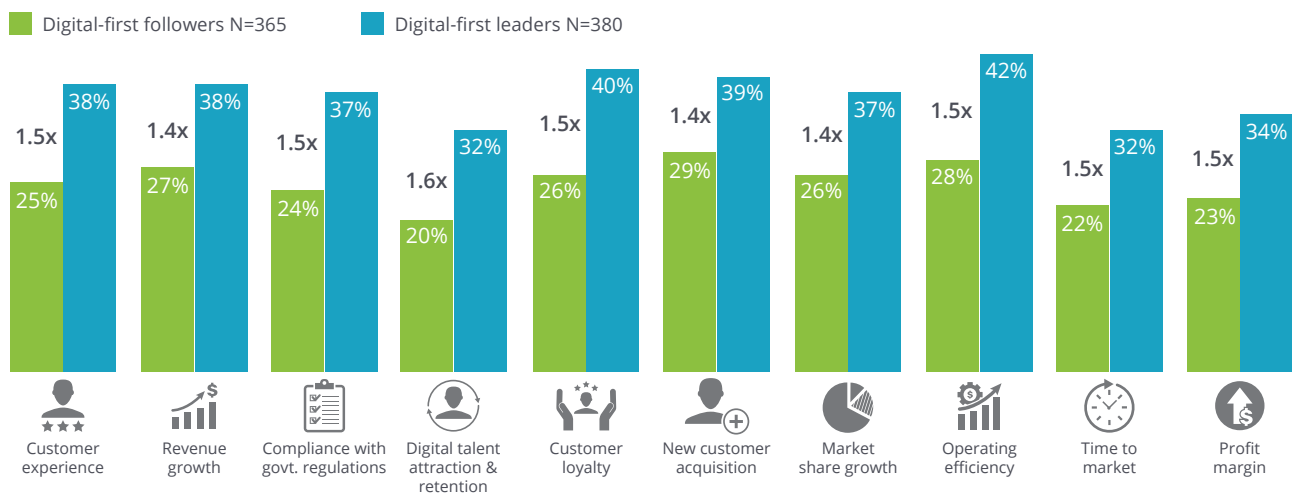
Upon further review, digital-first organisations with advanced CIAM maturity are 1.5x more likely to overperform their expectations in key metrics, such as new customer acquisition, customer loyalty, digital talent attraction and retention, and time to market for new products and services.

Figure 8: **Performance of key metrics**

Q. Measuring against internal expectations, how well do you think your organisation has performed in the following areas over the last 12–24 months?

% of organisations that overperformed against expectations

Digital-first followers N=365   Digital-first leaders N=380

Metric	Followers	Leaders	Ratio
Customer experience	25%	38%	1.5x
Revenue growth	27%	38%	1.4x
Compliance with govt. regulations	24%	37%	1.5x
Digital talent attraction & retention	20%	32%	1.6x
Customer loyalty	26%	40%	1.5x
New customer acquisition	29%	39%	1.4x
Market share growth	26%	37%	1.4x
Operating efficiency	28%	42%	1.5x
Time to market	22%	32%	1.5x
Profit margin	23%	34%	1.5x

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=745

SMBs versus enterprises

SMBs leverage enterprise-grade IT through SaaS ecosystem

Before the pandemic, most small and medium-sized businesses (SMBs) in Asia/Pacific had not embraced digital extensively, and adopted a reactive rather than a proactive approach towards digital transformation. Only 18% of SMBs had a digital-first strategy in place prior to the pandemic.
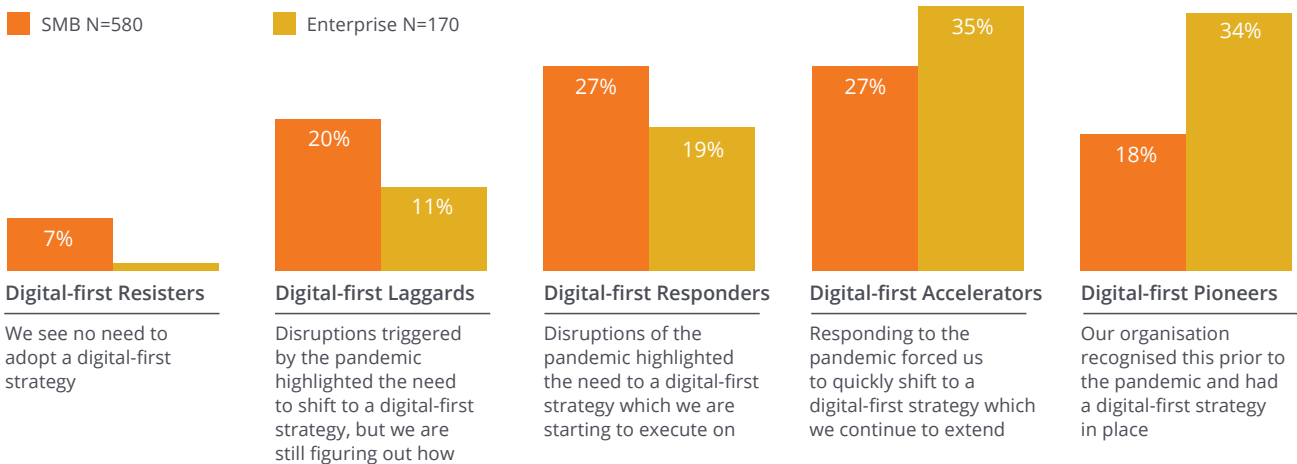
However, the past two years have brought about a mindset shift across SMB organisations. As a result of the pandemic-induced urgency, 54% of SMBs have started to shift to a digital-first strategy. SMBs understand the need to be a digital-first company and are ready to embed technologies to amplify their capabilities and enhance productivity, increase competitiveness, engage better with their customers and uncover more business opportunities through digital.

> **By 2024, 75% of start-ups will have a digital-first strategy, either adopting next-generation technologies, placing high emphasis on innovation, or focusing on digital disruption.**
>
> *— IDC's Worldwide Small and Medium-Sized Business 2022 Predictions – Asia/Pacific (Excluding Japan)*

Figure 9: Digital-first strategy adoption in SMBs versus enterprises

Q. Which of the following best describes your organisation?

	SMB N=580	Enterprise N=170

Digital-first Resisters	Digital-first Laggards	Digital-first Responders	Digital-first Accelerators	Digital-first Pioneers
7%	20% / 11%	27% / 19%	27% / 35%	18% / 34%
We see no need to adopt a digital-first strategy	Disruptions triggered by the pandemic highlighted the need to shift to a digital-first strategy, but we are still figuring out how	Disruptions of the pandemic highlighted the need to a digital-first strategy which we are starting to execute on	Responding to the pandemic forced us to quickly shift to a digital-first strategy which we continue to extend	Our organisation recognised this prior to the pandemic and had a digital-first strategy in place

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=750

The focus has clearly shifted to a customer-centric digital business model that augments the customer journey and creates a differentiated experience. While SMBs have benefited greatly from investments in a CX solution or platform, they are slightly behind the large enterprises with respect to securing customer data. The many challenges that SMBs face include lack of skill sets, manpower, budgets, technical expertise and adequate set of tools, thereby making them easy and soft targets for cyberattacks. A digital-first strategy therefore demands a fresh take on security, especially to secure customer data and identities. SMBs are still behind in CIAM adoption and only 45% have deployed a CIAM solution, compared to 57% adoption in the enterprise segment.

There is lower awareness among SMBs towards the need for CIAM platforms for a secure customer experience. More than 49% of SMBs still work with disparate and siloed CIAM technologies, instead of looking at a centrally governed CIAM, leading to internal challenges.
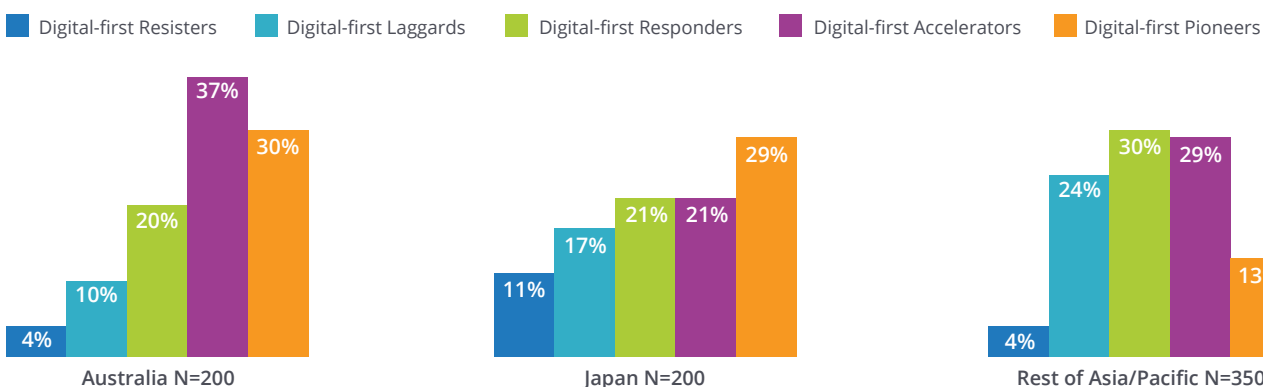
The digital-first SMB organisations are in the early stages of CIAM investments with technologies such as multifactor authentication, privacy consent management, and credential reset. However, they do have plans to move ahead in the journey with investments in more advanced technologies such as passwordless access, secure API access, and consumer-focused seamless authentication, in the next 12–24 months.

Even though more than 66% of SMBs surveyed acknowledge the importance and benefits provided by CIAM solutions, the struggle in terms of managing customer data and maintaining privacy regulations, securing systems from attacks, and integrating multiple touch points for easy customer access remain top concerns for SMBs in managing their CIAM journey. As a result, SMBs either collaborate with or outsource the CIAM management to third-party consultants or managed service providers, to design the right solution, provide support services, and manage/update the solution regularly.

Figure 10: **CIAM maturity – SMBs versus enterprises**

Q. Which of the following best describes customer identity and access management (CIAM) in your organisation?

SMB N=580   Enterprise N=170

Disparate — 49% / 30%
Enabled — 29% / 37%
Advanced — 21% / 33%
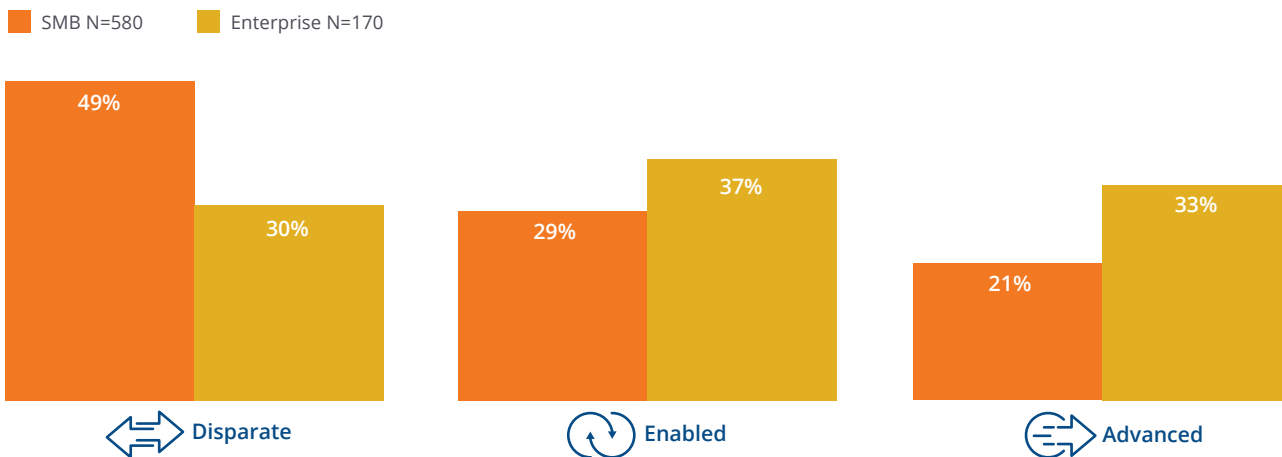
Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=750

CIAM around the Asia/Pacific region

Digitally mature countries are more focused on security and CIAM investments

Countries across the Asia/Pacific region fare differently in terms of digital maturity. Australia (67%), Singapore (66%) and New Zealand (60%) were the top 3 regions with a strong digital-first strategy in place. They displayed a stronger focus on CX investments as well as security and CIAM technologies which resulted in better performance across all operational and financial parameters.

Figure 11: **Digital-first strategy adoption in Asia/Pacific**

Q. Which of the following best describes your organisation?

Digital-first Resisters   Digital-first Laggards   Digital-first Responders   Digital-first Accelerators   Digital-first Pioneers

Australia N=200 — 4% / 10% / 20% / 37% / 30%
Japan N=200 — 11% / 17% / 21% / 21% / 29%
Rest of Asia/Pacific N=350 — 4% / 24% / 30% / 29% / 13%

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=750

Interestingly, regions with higher percentages of digital-first organisations are also more likely to consider CIAM as a top priority investment for their organisation. New Zealand (90%), Australia (87%) and Singapore (72%) were among the top regions that considered CIAM as a top priority.

Australia is one of the most mature markets with more than 70% of organisations viewing CIAM as a strategic investment, which is governed centrally and follows a platform approach for better visibility and enhanced experiences. They also work closely with service providers to manage their CIAM environment better.

Interestingly, Japan appears to be slightly lagging in its

CIAM maturity, with 50% of organisations viewing customer identities as single-purpose technology and have no or limited integration across other applications. As a result, they face challenges in integrating with internal systems and monitoring access privileges, and require assistance in designing the right solution for them and integrating it with other applications.

Other parts of Asia/Pacific have a maturing outlook towards CIAM adoption, with more than 68% of organisations considering CIAM as a top priority investment, and 48% are focused on common platforms that allow complete CIAM integration for a single pane of glass view.

Figure 12: **CIAM maturity across Asia Pacific**

Q. Which of the following best describes customer identity and access management (CIAM) in your organisation?

■ Australia N=200   ■ Japan N=200   ■ Rest of Asia/pacific N=350
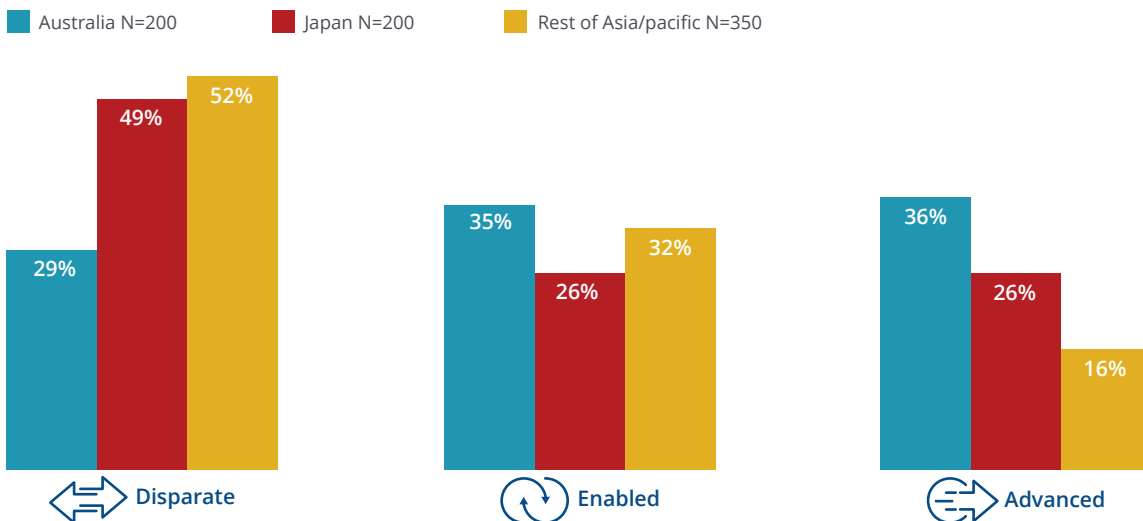
Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=750

IDC essential guidance

CIAM is a key component in executing a digital-first strategy. IDC's research shows that digital-first organisations are more likely to invest in more advanced CIAM capabilities and outperform in key customer-oriented metrics. The journey towards becoming a digital-first organisation is a challenging one. IDC recommends the following steps to navigate through the journey:

Guidance for Stage 1 (Disparate)

Align business goals with CIAM strategies: Develop a business case for enterprisewide CIAM and tie it with enterprise goals and objectives. Identify standards and frameworks related to customer identity management across different department functions and business units

Benchmarking: Evaluate the various CIAM technologies in use versus the current best practices across CIAM leaders and identify the gaps

Portfolio expansion: Expand from unified technologies such as MFA, privacy consent management, and unified user directory to more advanced CIAM technologies such as single sign-on for external users and automating provisioning/deprovisioning for employees and external users. Advanced CIAM technologies help provide contextual access to customers by taking into account various factors such as location and time of access, device being used, password strength to provide stronger identity security

Guidance for Stage 2 (Enabled)

Central management of customer data: Integrate applications and systems together such that customer information and identities are centrally stored and managed

Identity consolidation: Establish processes to manage multiple identity-based solutions under one common platform to enable better customer identity monitoring and analytics

Secure and seamless access: Leverage contextual access capabilities along with adaptive authentication such as passwordless access (biometric or push verification) and consumer focused seamless authentication to create a highly secure and frictionless experience

People and processes: To support a unified CIAM strategy, people and processes need to come together and work towards common business goals and objectives

Guidance for Stage 3 (Advanced)

Emphasis on building digital trust: Build a digital trust framework by adopting a security by design approach and create stronger customer engagement mechanisms

Greater use of analytics: Leverage analytics capabilities to identify new opportunities and revenue streams through digital products and services

Greater agility through embedded automation: Helps in compliance requirements as well, due to automation-enabled process efficiencies

Appendix: IDC methodology

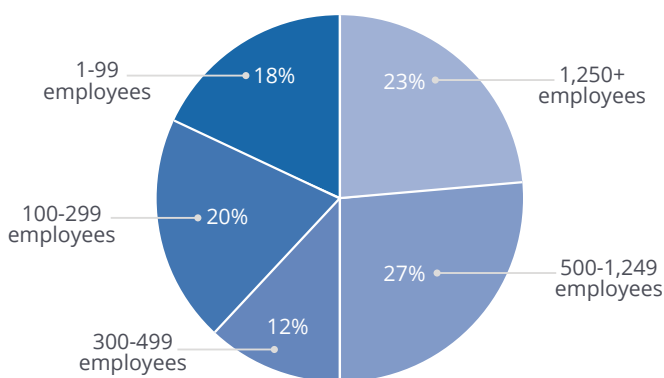## IDC's Asia/Pacific Customer Identity and Access Management Survey

The information presented in this White Paper is sourced from IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022. IDC surveyed senior and mid-level management in IT and lines of business across 750 organisations of all sizes and industries across Asia/Pacific. Survey respondents were asked about their organisations' business priorities, their current state, investment, and future intention in customer identity as well as business performance.

Figure 13: **Survey respondents' profile**

Respondents are solely/jointly responsible or have influence on security software-related decisions in their organisations.
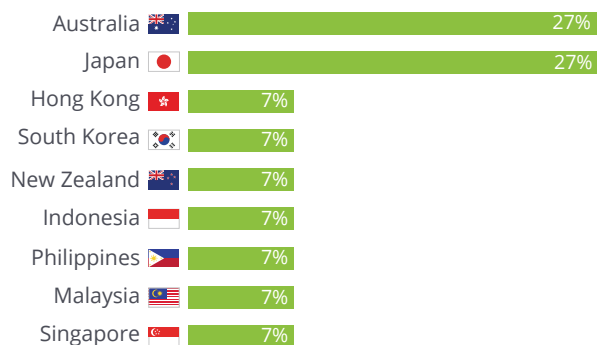
Company size

- 1,250+ employees: 23%
- 500-1,249 employees: 27%
- 300-499 employees: 12%
- 100-299 employees: 20%
- 1-99 employees: 18%

Target market

- Primary B2C: 50%
- Primary B2B: 50%

Job role

- Owner, C-Level, MD: 25%
- Dept. Head, VP, Director: 58%
- LoB or dept. mgr.: 17%
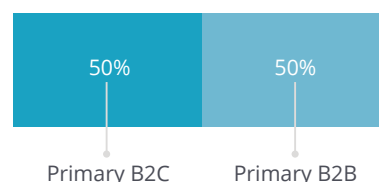
Job function/department

- IT/Eng.: 41%
- Sales & Mkt.: 13%
- Finance/Acct.: 14%
- LoB: 9%
- Operations: 13%
- Security: 4%
- Product Developer: 2%
- (top): 4%
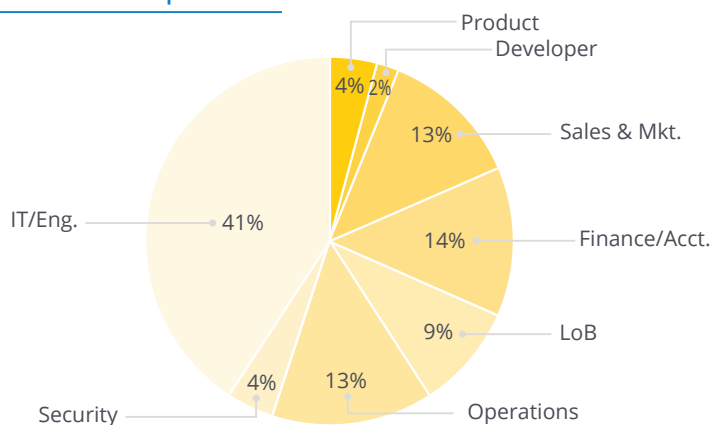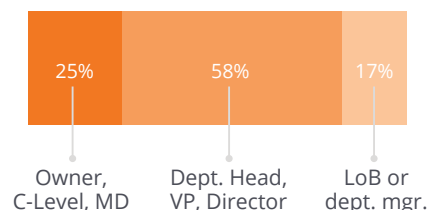
Industry/sector (self-described)

- Healthcare: 6%
- IT services: 6%
- Professional services: 6%
- Financial services: 6%
- Construction: 6%
- Education: 6%
- Manufacturing: 6%
- Tourism: 6%
- Distribution/logistics: 6%
- Retail: 6%
- Food: 6%
- Utilities: 6%
- Real estate: 6%
- Oil & energy: 6%
- Telecommunications: 5%
- Hospitality: 5%
- Transportation: 5%

Location

- Australia: 27%
- Japan: 27%
- Hong Kong: 7%
- South Korea: 7%
- New Zealand: 7%
- Indonesia: 7%
- Philippines: 7%
- Malaysia: 7%
- Singapore: 7%

Note: percentages might not add exactly to 100% due to rounding.

Source: IDC's Asia/Pacific Customer Identity and Access Management Survey, sponsored by Okta, April 2022, N=750

Message from the sponsor:

About Okta

At Okta we take customer identity off your hands, so your people can focus on doing what they do best.

The Okta Identity Cloud enables organisations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organisations everywhere, giving them the confidence to reach their full potential. More than 15,000 organisations trust Okta to help protect the identities of their workforces and customers.

To learn more, please visit -
https://www.okta.com/au/customer-identity/

okta

About the Analysts

Shweta Baidya,
Senior Research Manager, IDC Asia/Pacific

Shweta has over 10 years of experience in IT research and consulting, team management, business development, and client engagement. She is part of the software and IT services team in Asia/Pacific and is responsible for delivering syndicated, custom research reports and consulting projects on various categories under emerging and disruptive technologies.

Linus Lai,
Research Vice President, IDC Asia/Pacific

Linus Lai is the VP of IDC's Asia/Pacific Software and Services Research Group. He has more than 25 years of industry experience. Based in Sydney, he leads IDC's research programs in Security and Trust, Software and Services sourcing.

Linus is a founding member of IDC Global's Future of Digital Innovation Council and is on the judging panel of Australia's CIO50.

IDC

IDC Custom Solutions

IDC Asia/Pacific
83 Clemenceau Avenue,
#17-01 UE Square West Wing
Singapore 239920
T 65.6226.0330

Twitter @IDC
idc-community.com
www.idc.com

The content in this paper was adapted from existing IDC research published on www.idc.com.