

State of Identity in Asia/Pacific - 2022

Introduction

2021 witnessed a significant acceleration in digital transformation initiatives across enterprises, to deliver new customer experiences as well as transform back-office operations with intelligent automation technologies. Digitally mature organisations were quick to adapt in this work environment and took a "digital-first" approach in every facet of their business, recognising that in a digital-first economy, software capability — augmented by AI and pervasive computing — could drive new purpose, innovation, and sustainability in the long term.



IDC predicts that by the end of 2022, half of the Asia/Pacific economy will be based on or influenced by digital technologies. As a result, organisations in the region will increase leverage of digital technologies to address the rapidly evolving needs of work (i.e., hybrid-first), deliver consistent customer experiences across digital and physical channels, achieve operational autonomy, and become intelligent enterprises.

However, the transition to hybrid work models has resulted in a steady rise in the attack surface and associated risks, leading to greater focus on security investments across Asia/Pacific enterprises. The need to tightly secure both on-premise and cloud environments became a primary objective. The topmost concern that enterprises face today is how to secure data, networks, and users in an environment where the threat landscape continues to expand and multiply.

Data regulation and legislation across the region also act as a key driver for security adoption, but it is often a patchwork across the regions with no homogenous standards. Markets such as Australia, New Zealand, Singapore, and, to a degree, Hong Kong, subscribe to relatively stringent data privacy and breach notification legislation, whereas others have either little or a limited patchwork of legislation that is difficult to enforce. Last year marks the first time in a long time, that IDC has seen a return to federated identity and privilege management to strengthen access credentials, through common standards and frameworks for easy authentication and authorisation processes. We expect this trend to continue in 2022.

State of identity management

Identity management solutions have become the cornerstone to manage user identities better. As per IDC's Asia/Pacific (AP) Security Services Survey conducted in 2021 across 879 organisations in the Asia/Pacific region, identity security was the top area of focus for more than 40% of organisations surveyed. Although most enterprises have already implemented low-hanging opportunistic and incremental technologies such as multifactor authentication, as per IDC's Future Enterprise Resiliency and Spending (FERS) Wave Survey conducted in December 2021, about 80% of enterprises intend to continue to retain or increase their spending in advanced authentication/multifactor authentication during 2022.



Further gains can be achieved through technologies such as contextual access control (e.g., passwordless solutions) and using a combination of analytics, AI, and ML to detect anomalous behaviour across users, devices, applications, and infrastructure. Identity governance and privileged access management are considered essential/critical towards maintaining identity hygiene.







IDC also expects a greater adoption rate of biometric authentication technology across all identity segments i.e. business-to-employee, business-to-business, and business-to-consumer (B2E, B2B, and B2C) to help governments, enterprises, and users improve access speed, user authentication, and overall experience. However, what stood out as a clear differentiator during the pandemic was B2C identity management, which witnessed the strongest growth of 31.4% across APJ during FY 1H21.

It is now a fundamental factor for the success of business operations moving forward that identity management on the cloud is an essential building block towards achieving complete digital trust. Digital trust is all about building credibility across your entire ecosystem including customers, partners, suppliers, and internal stakeholders.

As a result, enterprises are evaluating zero trust frameworks as an alternative to provide a comprehensive and secure work environment. In a zero-trust design, the identity of every user, device, and network is authenticated and verified before providing access. While planning a zero-trust strategy, identity is at the core of the entire blueprint of security architecture, as it provides the additional layer of security in an increasingly perimeterless yet connected business world and forges digital trust across the ecosystem.

IDaaS building momentum: key drivers

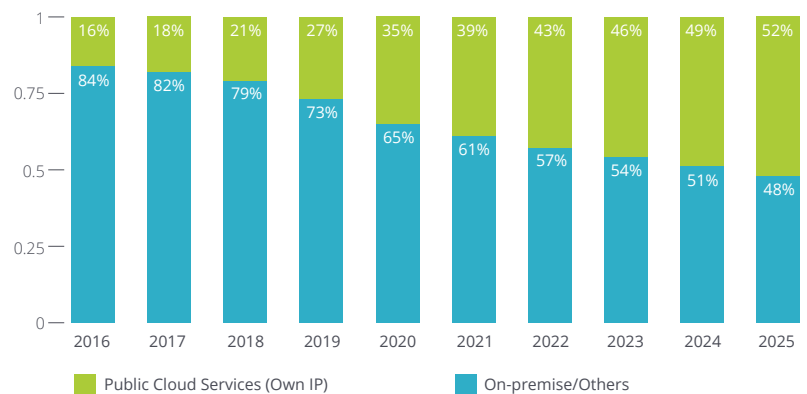
As organisations move to a cloud or mobile-first environment, the need to simplify and unify operational approaches become pertinent. Challenges such as data sovereignty requirements, the need for a centralised directory for hybrid datacentre environments, and evolving identity management needs have driven significant momentum in the adoption of an identity as a service (IDaaS) or cloud-based authentication model that provides distinct benefits:

 <p>Cost savings, operational efficiency, and expertise bundled together</p>	 <p>Shorter time-to-value as identity experts do the work</p>	 <p>Support identity federation standards such as Security Assertion Markup Language (SAML), Open Authorisation (OAuth) that allows users access with a single set of credentials</p>	 <p>Single sign-on and multifactor authentication that are readily available</p>	 <p>Eases task of managing ever-increasing data sovereignty and privacy requirements</p>	 <p>Centralised directory for hybrid datacentre environments</p>
---	--	--	--	---	---

Future of identity: building a unified platform

Many organisations now believe that security as a service is the best way to deliver outstanding functionality and manageability. IDC's Identity and Digital Trust Software Market Forecast shows that IDaaS is set to overtake traditional modes of software deployment by 2025, in a number of countries including India, South Korea, Malaysia, New Zealand, and Singapore, due to the cost benefits, flexibility, and ease of deployment, among other reasons.

Identity & Digital Trust Software Market Forecast, 2020-2025



Source: IDC Semiannual Software Tracker, 2021H1 Forecast

IDaaS can help to solve the problem of too many legacy point solutions with an identity platform that can integrate across a broad range of use cases, remote access, and dominant cloud services integration in the future. As organisations progress in the maturity curve, an identity and access solution is likely to be better integrated with other areas of IT operations and management and various security modules such as MDM, SIEM, automation, to build a more unified and streamlined security operation system. As a result, vendors who build and provide identity security platforms that offer an end-to-end solution, both on-premise as well as in the cloud, will become the preferred partners of digital enterprises in the future.

Message from sponsor:

As a leading independent identity provider, Okta 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. More than 14,000 organisations trust Okta to help protect the identities of their workforces and customers. [Get in touch](#) to learn more.

