Focus on Australia and New Zealand

2024/25 Tech Insider

Introduction

Digital native businesses (DNBs) were born in the internet era and are built around the latest available technologies at birth.

Unencumbered by legacy technology and processes, digital natives — across a wide swathe of industries such as gaming, retail, and education — move at the speed of tech to keep up with customers' demand to work, live, and play online.

According to technology research firm IDC, DNBs are forecasted to spend up to $128.9 billion on technology by 2026.

In March through May 2024, Akamai conducted an online survey with third-party research firm TechnologyAdvice to find out the technology investment priorities of DNBs across Asia and what keeps their tech leaders up at night.

More than 200 tech leaders responded to the survey across Australia, New Zealand, Southeast Asia, India, and Greater China.

The survey found that nearly 9 in 10 DNBs surveyed are prioritising efficiency and productivity in the next 12 months.

This corroborates industry data showing rapid cloud adoption among DNBs. The 2021–2026 estimated growth rate for tech spend on cloud-based solutions is 37%, ahead of non-cloud software (16%) and IT services (11%).

This cloud-native modular architecture built around microservices that operate independently and communicate through APIs enables DNBs in this region to rapidly scale and meet rising customer digitalisation.

However, this can very quickly become a complex matrix of software, systems, and services that threatens to expose DNBs to greater cyber vulnerability.

Regardless of where they are in their cloud journey, DNBs in the region are acutely conscious that security is the biggest gap in their cloud infrastructure's performance.

In fact, their increasingly complex IT infrastructure may prove to be the Achilles' heel in enhancing their cybersecurity posture, as a majority cite this challenge ahead of budget or compliance issues.

Such growing pains around increasing tech complexity may also be a cautionary tale for those considering cloud adoption or looking to migrate further into the cloud.

This excerpt focuses on the tech priorities and challenges, particularly of DNB respondents in Australia and New Zealand.

Australia/New Zealand: From start-up to scale-up

The post-Covid economic headwinds in Australia/New Zealand (ANZ) have yet to ease off, and customers are facing financial pressure with slow wage growth and persistent inflation.

Analyst reports point to weak domestic demand and soft labour demand in the coming years.

Perhaps in response to the current economic climate, survey respondents from ANZ are prioritising efficiency and organisational resilience.

There has also been a mindset shift as cloud tech now becomes a business essential. Ninety-seven percent of respondents have either embraced cloud or are exploring cloud adoption.

Compared to respondents in other markets, ANZ organisations are moving further along the cloud adoption curve to further extract operational efficiencies in a cooling economy.

Summary of key forecasts

Calendar Years	2020	2021	2022	2023	2024f	2025f	2026f
Real GDP[1] (annual average % change)	-1.4	5.6	2.4	0.6	0.5	1.5	2.5
Unemployment rate (sa; Dec qtr)	4.9	3.2	3.4	4.0	5.1	5.5	5.0
CPI inflation (annual % change; Dec qtr)	1.4	5.9	7.2	4.7	2.6	2.0	2.0
Official cash rate (Dec qtr end)	0.25	0.75	4.25	5.50	5.50	4.75	4.00

[1] Production based

Source: Statistics NZ, REINZ, Bloomberg, ANZ Research

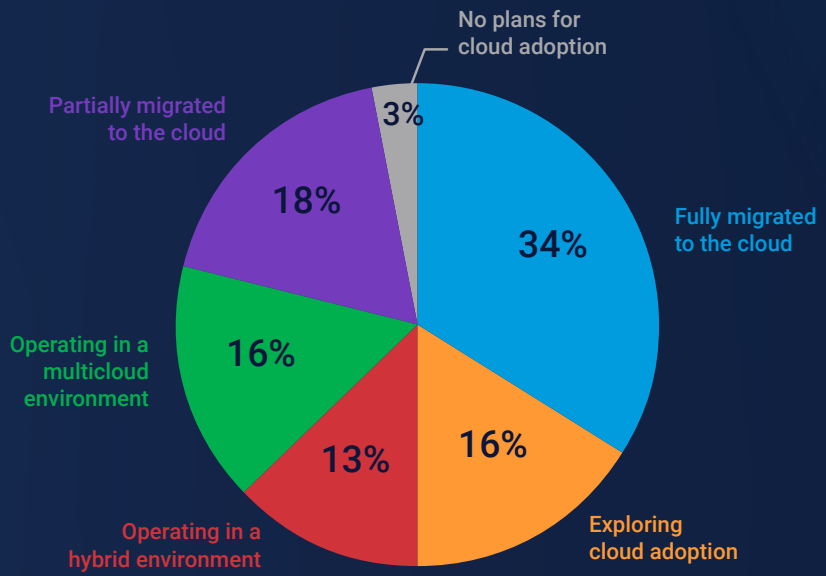
Top business priorities in the next 12 months

A higher proportion (81%) of ANZ's respondents have embraced cloud technologies either with full, partial, or hybrid cloud adoption.

For example, ANZ's public cloud adoption has moved beyond discrete software as a service–based solutions for infrastructure replacement, like disaster recovery, to advanced use cases driving organisation-wide digital transformation and innovation.

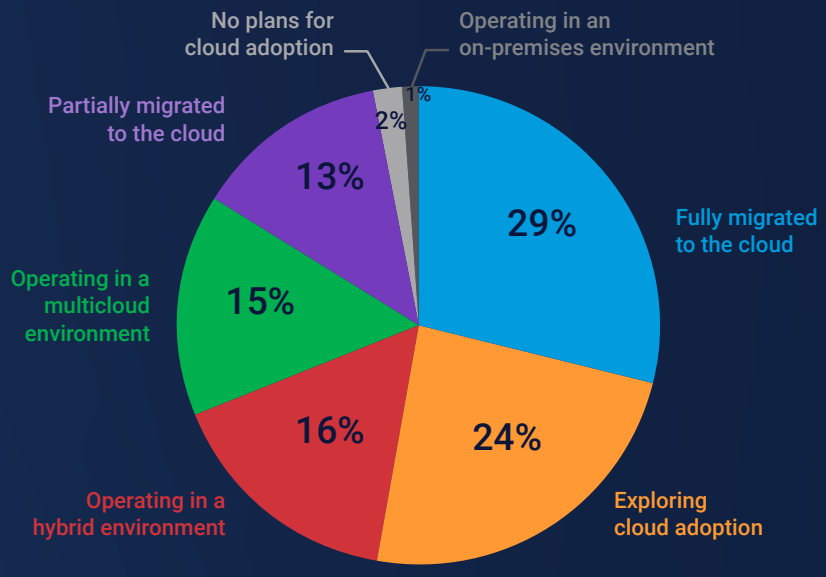
This relative cloud adoption maturity has seen a mindset shift from cloud as a business disrupter to cloud as a business essential.

At what stage is your organisation in its cloud adoption journey?



Cloud adoption in ANZ

At what stage is your organisation in its cloud adoption journey?



Cloud adoption across APJ

Australia's MiClub scales up with cloud migration

More than half of Australia's 1,500 golf clubs use MiClub's golf and club management solutions.

The company is also making inroads into other global regions by using its subscription-based model to help support exponential growth.

MiClub, driven by a commitment to service excellence and technological advancement, recently migrated its infrastructure to the cloud to enhance scalability and customer experiences.

By transitioning from a traditional data centre setup, MiClub optimised flexibility and performance to accommodate the fluctuating demand from golf clubs.

Amid a surge in business during the COVID-19 pandemic, MiClub seamlessly migrated to Akamai's cloud computing services, enabling scalable solutions tailored to individual club needs. With its ongoing expansion efforts and more than 1,100 deployed nodes, MiClub recognises the need for flexible infrastructure to handle daily spikes in demand.

MiClub sought solutions to streamline the processes for its golf and club management systems. The intense demand, particularly for coveted tee times, required robust and scalable systems.

Players' use of various devices amplified the need for a seamless booking experience. MiClub's transition to Akamai addressed these challenges, ensuring smooth operations and enhancing customer satisfaction. MiClub harnesses Akamai's transparency and support to deliver exceptional service to its growing clientele.

"We chose Akamai due to ease of use, cost, and the fact that Akamai is a massive supporter of the Linux community," said Paul Dean, IT Manager, MiClub.

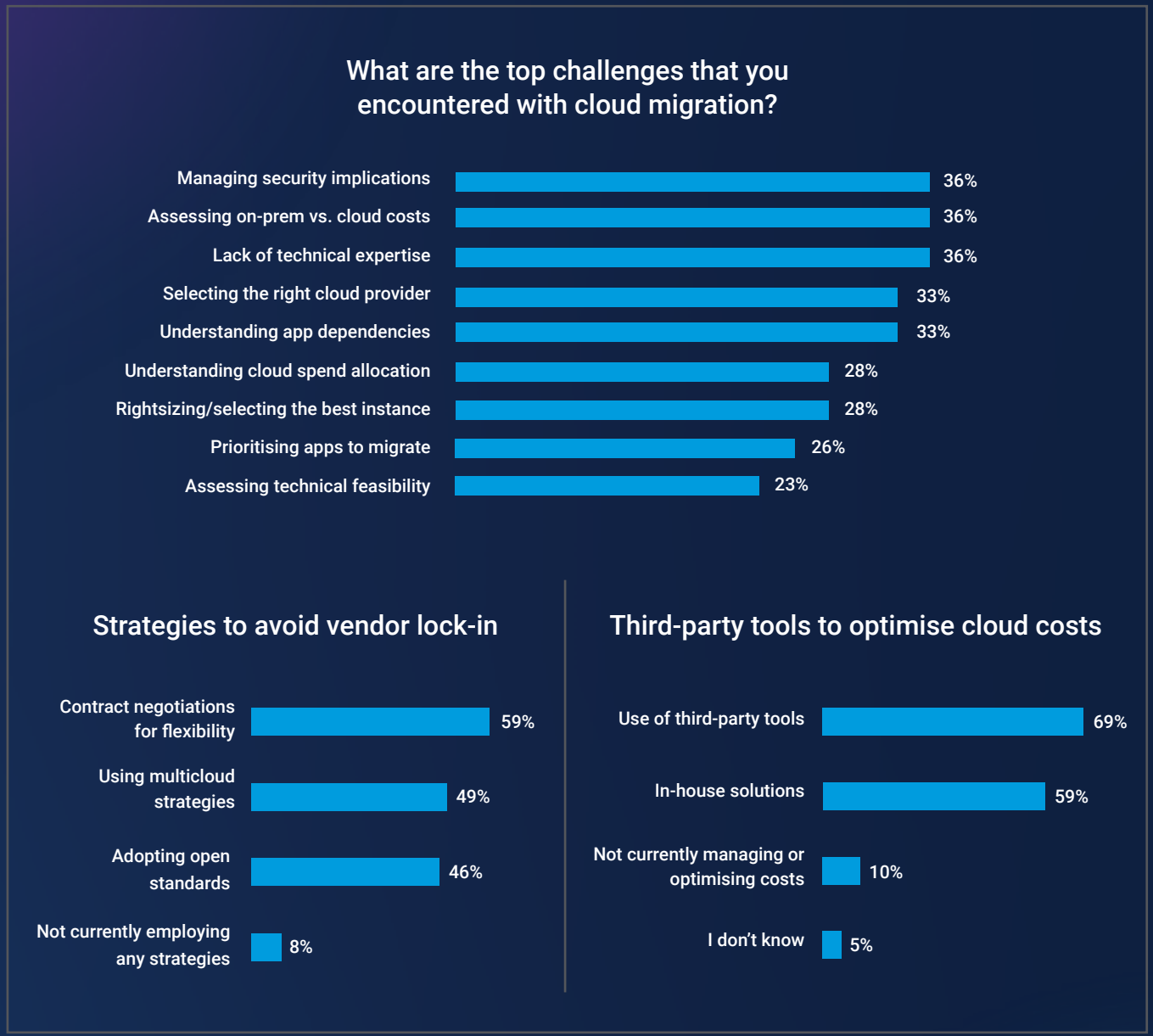
The public sector is also a dominant force across cloud adoption in both Australia and New Zealand, with the latter tabling a cloud-first government policy in 2012 and Australia doing so in 2015.

Australian companies are estimated to spend US$15.4 billion on public cloud in 2024, up 19.7% from 2023 (source: Gartner).

At the same time, being further along the digital adoption curve means that ANZ organisations may have legacy applications that are not architected for the cloud, not containerised, or not microservices based — and end up costing more than cloud-native applications.

ANZ survey respondents cite cloud costs as one of the top challenges encountered with cloud migration, along with managing security implications and the lack of technical expertise.

In fact, the scale of tech adoption, combined with innovation pressure and an economic slowdown, has revived interest in minimising cloud waste.



Cloud costs can be complex because of the expertise and time required to predict and decipher the costs for micro-services and multicloud deployments that all scale differently based on various factors.

This is where cloud cost management solutions such as FinOps introduce financial accountability to the cloud's variable spend model.

Various cloud users across the organisation can thus be held accountable for spend decisions with visibility into the overall cloud usage and possible productivity optimisation opportunities.

According to the survey findings, ANZ's IT leaders are leveraging contract negotiations with higher amounts of committed spend or larger committed growth rates in exchange for discounts.

This also points to relative cloud adoption maturity as ANZ respondents leverage third-party tools and managed services to augment dedicated staff for efficient, sustainable scale.

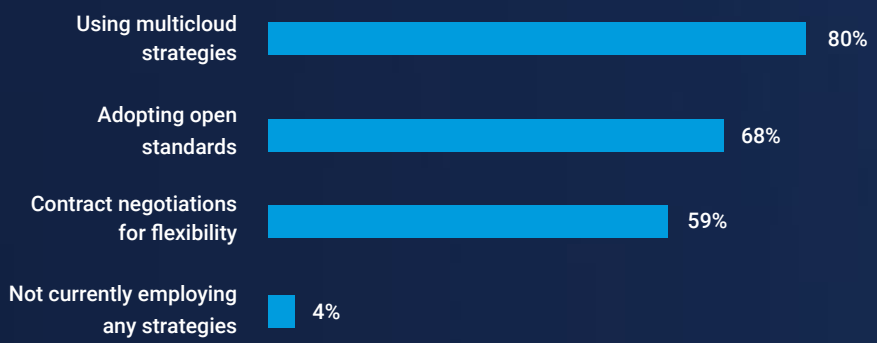
In comparison, respondents in India and ASEAN prefer deploying multicloud strategies and adopting open standards to avoid vendor lock-in.

Combining cloud operations management with financial governance can protect the organisation against unrestricted autoscaling that may consume your annual cloud budget overnight.

> ***Akamai's global network is integrated into 1,200 networks around the globe, and maintains optimised interconnects with all major cloud providers to ensure high availability, low latency, and infinite scale.***

India: Strategies to avoid vendor lock-in

ASEAN: Strategies to avoid vendor lock-in



Richer customer experience means more sensitive data

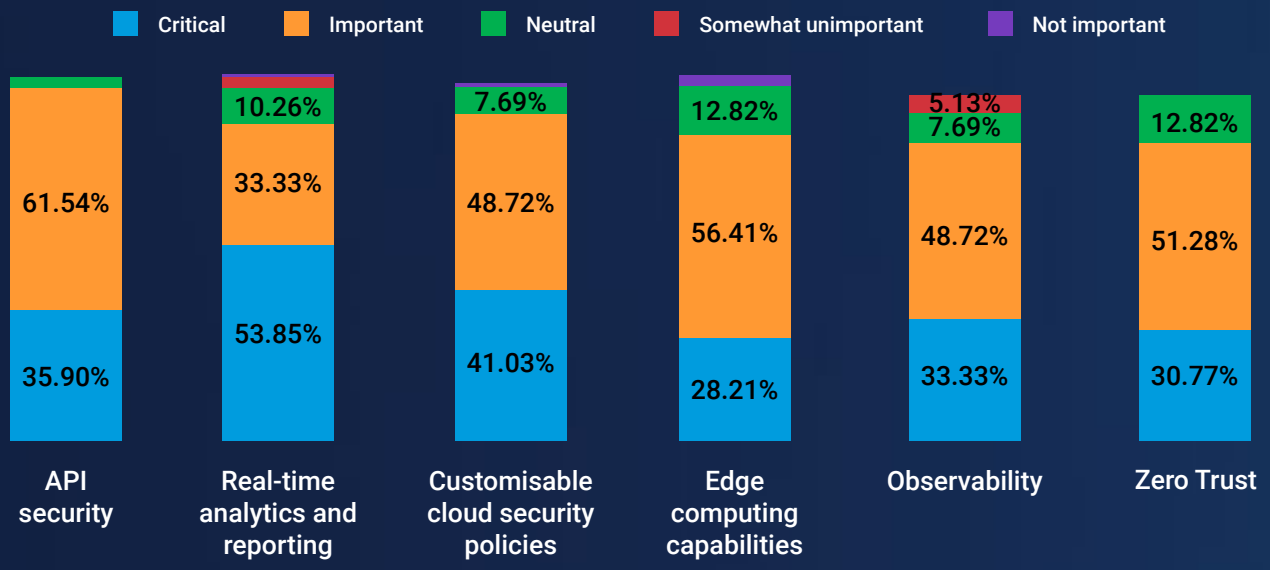
With a relatively mature customer digital adoption, ANZ businesses want the ability to ingest, process, analyse, and act on real-time data to provide an optimal user experience.

Eighty-seven percent of ANZ respondents marked real-time analytics and reporting as a critical/ important product feature in their evaluation of a cloud/security solution provider.

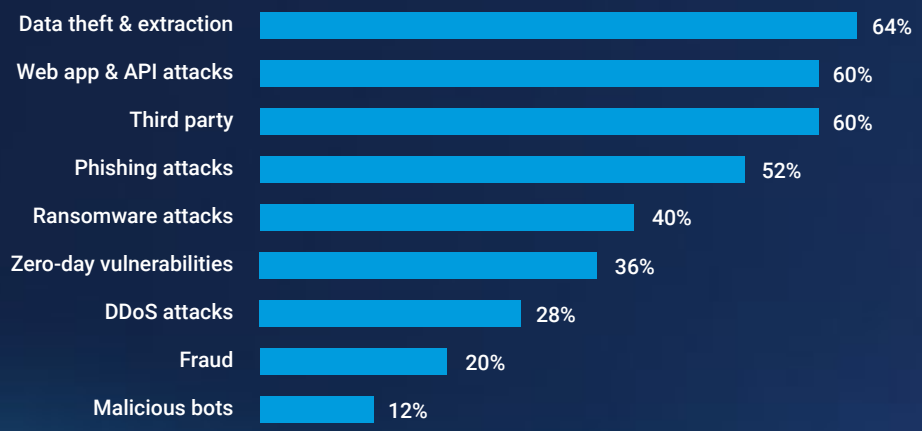
At the same time, the pursuit of richer customer experiences among ANZ digital natives also risks exposing them to cyberattacks targeting rich personal and financial data.

Web app and API attacks together with data theft and extraction were among the top cyberthreats of concern for IT leaders in Australia, according to Akamai's Cybersecurity in Financial Services report.

How important are the following product features in your evaluation of a cloud/security solution provider?



Top cyberthreats of concern for IT leaders in Australia



There is a security dimension, as ANZ IT leaders feel that the biggest issue they face around API security is visibility to API attack activity (20%) and adapting protections to evolving API attacks (24%).

As the adage goes: You can't protect what you can't see. Many companies aren't even aware of how many APIs they truly have, so it becomes difficult to quantify their risk.

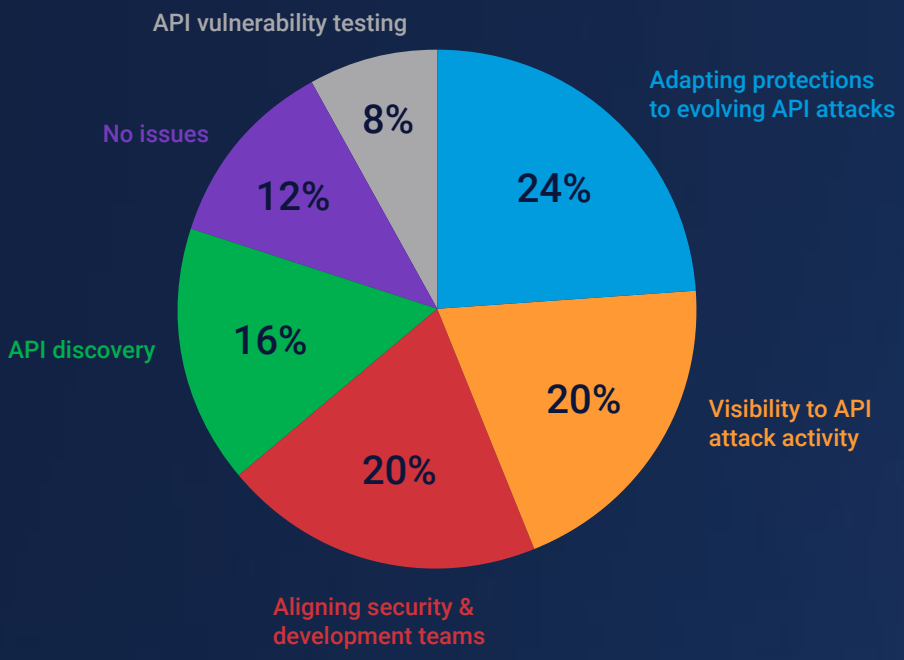
One of the biggest surprises for many enterprises that increase their visibility into API activity is the number of shadow endpoints that were unknowingly operating in their environment. Shadow endpoints are web services endpoints that are either outdated or undocumented, and thus not actively managed.

As a result, API security is marked as a critical/important product feature when evaluating cloud/security solution providers for 97% of ANZ respondents.

For many organisations, APIs now serve as the connective tissue that brings application functionality and data together to power critical business processes — both internally and with partners. This shift has unlocked many new business opportunities across a diverse set of industries. But it has simultaneously created an entirely new set of challenges for enterprise security teams.

This is where real-time analytics and reporting can enable faster detection and response, and reduce the damage in the event of a cyberattack.

What is the biggest issue you face around API security?



Early efforts by security teams to adapt to the API wave largely followed the traditional enterprise security playbook: Analyse events in the moment, respond based on predefined policies, and move on.

This approach has the benefit of immediacy, but it falsely assumes that all attacks (a) have been seen before, and (b) are executed as a single-point-in-time event.

This approach also leaves security teams with a data-poor API security model that is incapable of detecting the more sophisticated API attacks that unfold in small steps over a longer period. In effect, everything that is detected is immediately forgotten.

Evolving to a data-rich security approach that can form a deeper understanding of normal behaviour and detect behavioural anomalies is the most effective way to stay a step ahead of today's ever-evolving API threats.

Although implementing data-rich API security on your own might seem daunting, Akamai makes adding these capabilities to your overall security strategy faster and easier.

Even as the industry landscape continues to evolve and increase in complexity, Akamai seeks to accelerate the ambitions of ANZ's digital businesses without compromising their security posture.

Conclusion

The survey offers groundbreaking insights into the challenges faced by tech leaders in Australia as they embrace AI, cloud computing, and big data in pursuit of richer and faster customer experiences.

The research distinguishes the nuances in cloud/API maturity and cybersecurity posture of digital natives in various geographies and industries across Asia-Pacific.

For example, those in highly regulated industries or geographies like in Australia are looking to balance security and privacy with the user experience.

At the root of it all, cloud-native architectures benefit from well-architected APIs and endpoints that enable digital natives to scale up/out and deliver rich, personalised experiences.

Most organisations lack the native visibility and security controls required to effectively lock down a cloud.

For public and multicloud environments to be secure, security practitioners must be able to see which applications, workloads, and traffic flows are moving within the environment.

Akamai is changing how organisations approach cloud architecture, emphasising a more distributed, decentralised, low-latency, and globally scalable design — ideal for higher-performance workloads that need to run closer to end users.

Our push to establish core compute regions in hard-to-access markets around the world has seen a massively distributed footprint spanning more than 4,200 edge PoPs across more than 130 countries.

Talk to us and find out why leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences.

Methodology

The survey uncovered these insights with on-the-ground research of IT leaders across the region. It was conducted March–May 2024.

Why

The report looks under the hood to understand how digital native businesses view upcoming trends and threats. These findings serve as an invaluable benchmark built on current on-the-ground insights.

Who

Chief information officers, chief technology officers, IT directors, and VPs of the following industries:

- Airlines
- Media/broadcast/publishing
- Ecommerce/internet
- Gaming
- Hospitality
- Information technology
- Retail/wholesale

Where


Australia


New Zealand


India


Singapore


Indonesia


Thailand


Malaysia


Vietnam