Focus on ASEAN

2024/25 Tech Insider

Introduction

In March through May 2024, Akamai conducted an online survey with third-party research firm TechnologyAdvice to find out the technology investment priorities of digital native businesses (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.

What are Asian DNBs' business priorities and technology concerns? What do these tech-driven companies look for in their solution providers?

Whether it is due to maturing market competition or a fast-growing consumer base, nearly 9 in 10 DNBs surveyed prioritise efficiency and productivity in the next 12 months.

This corroborates with 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.

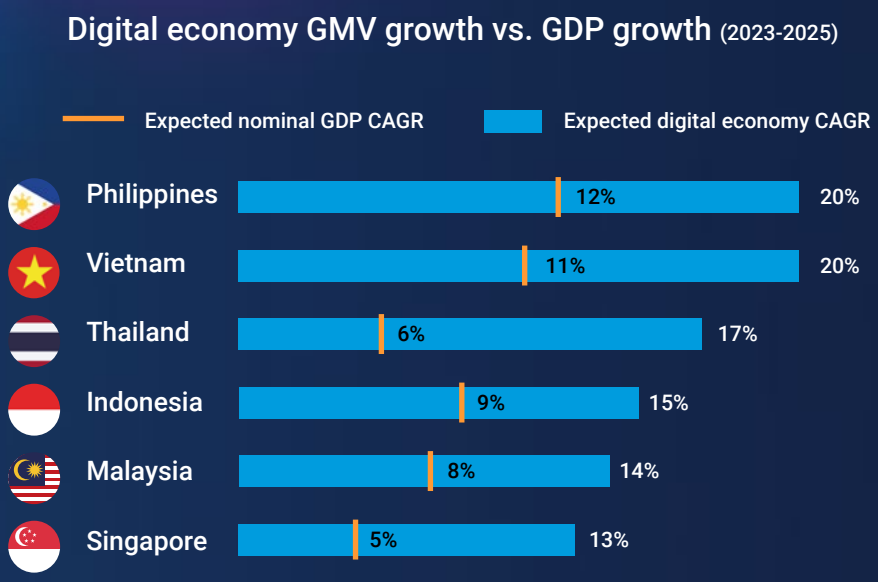
This excerpt focuses on the tech priorities and challenges, particularly of DNB respondents across Southeast Asia.

Connecting ASEAN: Digital economy drives region's growth

Southeast Asia is the fastest-growing internet market in the world, with 125,000 new users coming on the internet every day (Source: World Economic Forum).

Digitally native and connected millennials and Gen Z are expected to account for 75% of ASEAN consumers and 70% of Indonesian consumers by 2030 (Source: World Economic Forum).

In fact, the region's digital economy gross market value growth exceeds that of GDP growth across all ASEAN countries (Source: e-conomy SEA 2023).



(Source: e-conomy SEA 2023, Google, Temasek, and Bain & Company)

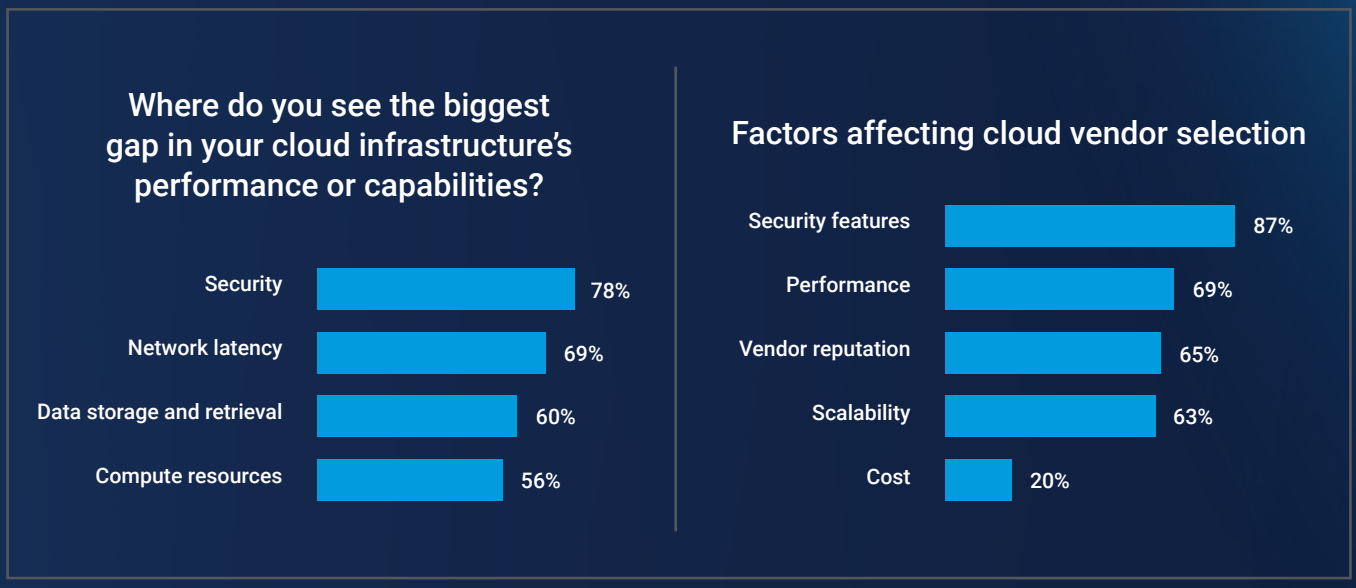
Cloud security gaps

Security remains top of mind among ASEAN respondents. More than three-quarters of respondents in the region cited security as the biggest gap in their cloud infrastructure's performance or capabilities.

It was also a top factor for 87% of respondents when selecting a cloud vendor.

When moving to the cloud, modern enterprises encounter an increasingly complex security challenge.

They're still facing the threats of ransomware and other security attacks, but neither the cloud-native security tools nor their legacy firewall tools can cater to the unique challenges of the cloud.



In particular, they're experiencing:

1 Poor visibility

The visibility provided by the cloud provider is based on raw logs that inventory the flows between different workloads. Without integrating those logs into a third-party system that provides clear understanding of the application dependencies and how the applications communicate, it's extremely complex to determine what policy you need to apply to your applications.

2 No single, consistent policy

Creating consistent policies across hybrid cloud environments using native cloud security tools is extremely complex. Microsoft Azure, for example, holds multiple subscriptions, each subscription having its own objects and rules — and therefore its own policies that are not shared across the different regions. This makes it extremely difficult to see the big picture.

3 Decentralised governance

The third challenge is operational: How do we connect the security policy to the actual DevOps operations? With application owners creating the application infrastructure as code, the security team is facing the challenge of how to work with this new concept (infrastructure as a code) and still maintain the network security posture.

The result is weak security in cloud environments — and attackers know it.

According to IBM's Cost of a Data Breach Report 2024, 82% of all the breaches reported last year involved data stored in the cloud — public, private, or multiple environments. Even worse, the report found that 39% of those breaches spanned multiple environments, incurring a higher-than-average cost of US$4.75 million.

Keeping ASEAN connected

At the same time, the region's infrastructure still needs to keep up with an increasingly digital ASEAN consumer base.

The digitally savvy younger generation has high expectations for service uptime and low latency.

It is to be expected that performance and vendor reputation rank highly, at 69% and 65%, respectively, for vendor selection among the ASEAN respondents.

More than two in three respondents also cite network latency as a gap in their organisation's cloud infrastructure performance and capabilities.

Digital native businesses that are quickly adopting a distributed cloud approach are those in industries that have urgent needs for low latency, such as gaming, media, and retail.

These are the customers with large bandwidth considerations, where they don't necessarily want to move large amounts of data back to a centralised server and want to be able to act on that data where it's collected.

It is thus not economically feasible for organisations to try to transmit all that data back to a centralised cloud, since they'll be paying for data storage as well as ingress and egress bandwidth.

> ***Akamai provides infrastructure in more regions than other providers, cloud computing resources at the core and the edge, and the ability to power and globally scale low-latency, data-intensive applications designed to satisfy regional preferences.***

API security a critical product feature for ASEAN

ASEAN DNBs are painfully aware that APIs keep their organisations running and help to facilitate collaboration with other vendors and ecosystem partners.

APIs are at the heart of most of today's digital transformations, so understanding industry trends and relevant use cases (e.g., loyalty fraud, abuse, authorisation, and carding attacks) is paramount.

ASEAN respondents have the highest confidence (99%) in recognising and mitigating advanced API attacks compared to their peers in ANZ (69%) and India (91%).

In fact, API security is marked as critical/important for nearly all (99%) of the ASEAN respondents.

However, API sprawl is real, and the fast speed of growth means lack of visibility, which can quickly become a security and compliance issue.

Visibility is a critical aspect of API security. Once blind spots like shadow APIs or rogue APIs are illuminated, security teams can start to address vulnerabilities that they were previously unaware of.

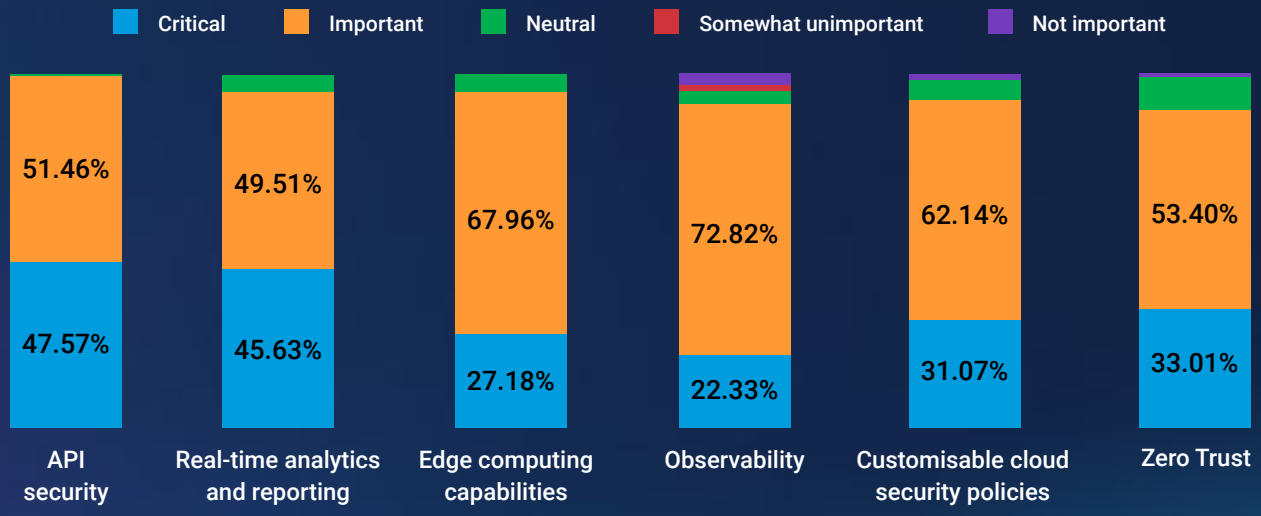
Hence, real-time analytics and reporting are rated as critical/important for 95% of the ASEAN respondents.

Without proper care, APIs can become a rich source of data breaches, compliance violations, and lapses in governance.

How confident are you in recognising and mitigating advanced API attacks like those in OWASP API Top 10?

Geography	Confident/Very confident
ASEAN	99%
ANZ	69%
India	91%

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



Unprecedented digital growth brings out phishing concerns

The high digital adoption rate has become a double-edged sword for ASEAN's DNBs.

Digital adoption is happening at such a fast rate that privacy is not necessarily at the forefront of customers' minds when they exchange information online. Phishing has evolved from an email-based attack to one that now includes mobile devices and social media.

As a result, the region has seen one of the highest levels of phishing, with nearly 500,000 reported cases in 2023 alone.

Data protection and privacy laws across ASEAN are very much dependent on the respective governments' ability to keep up with fast-changing digital communication trends. For example, clickable links in text messages are still a popular scam tactic, although more countries are implementing policies to block this common phishing method.

The surveyed ASEAN DNBs place a high priority on investing in anti-phishing technologies ahead of their peers in the region:

Detected and blocked financial phishing attacks in Southeast Asia in 2023

Country	Number of financial phishing attacks
Philippines	163,279
Malaysia	124,105
Indonesia	97,465
Vietnam	36,130
Thailand	25,227
Singapore	9,502
Total:	455,708

Source: Kaspersky, 2024

Rank the following cybersecurity investment areas from most important to least important

1. Anti-phishing technologies
2. Advanced API security
3. Web application security
4. Zero Trust–related technologies
5. Distributed denial-of-service (DDoS) mitigation

Phishing is the oldest and wisest attack vector.

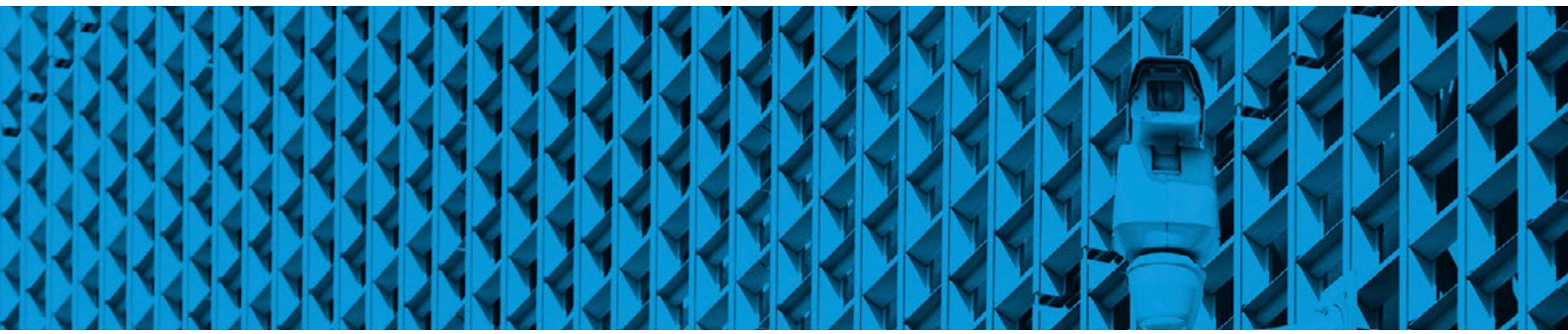
The rise of generative AI will make phishing attempts more convincing and open more options for criminals to target their victims. After all, phishing focuses on human nature instead of software vulnerability or system exploit.

This is where a good offence is good defence. Phishing simulations, combined with solid endpoint protection, can help DNBs stay ahead of the phishing game.

Trying to stop phishing permanently is a fool's errand — people will always click a link or have their curiosity piqued by something.

Instead, focusing on detection, and decreasing the lifespan of a given phishing kit's deployment is an obtainable win in the security space. Because phishing isn't just an email problem, defences will have to exist outside the inbox — which is where awareness, proactive scanning, and kit-based instead of domain-based fingerprinting come into play.

IT leaders will need to be thoroughly familiar with the threat and make sure we know more about the walls being built by threat actors to make sure we're not staying outside of the fence, while pursuing digital innovations.



Conclusion

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

For digital natives where milliseconds matter, cutting-edge capabilities that enable personalised experiences with hyperlocal optimisations are paramount.

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 4,100 edge PoPs across 131 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 in 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