Asia's Digital Native Businesses Prioritise Security for Sustainable Growth

2024/25 Tech Insider

Executive summary

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 customer 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, 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? Are all digital natives cut from the same cloth?

Whether it is due to maturing market competition or a fast-growing consumer base, nearly 9 in 10 DNBs surveyed will prioritise 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.

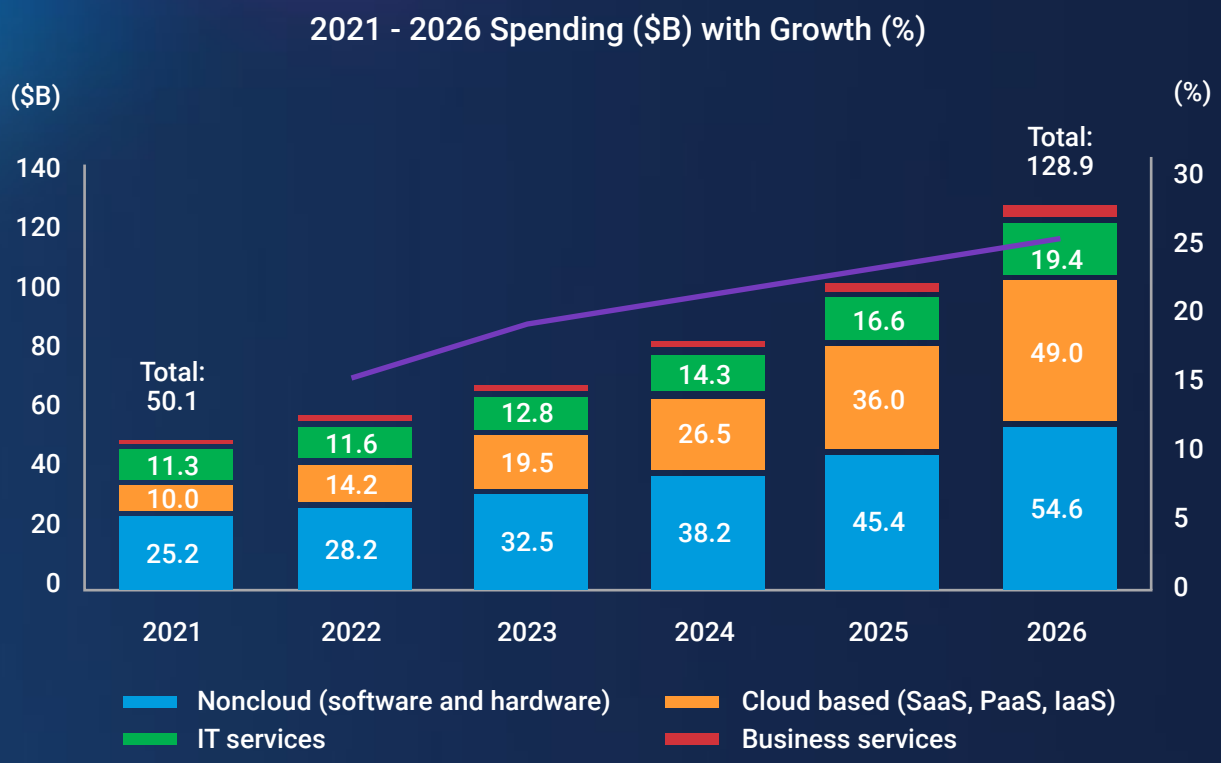
Find out actionable strategies to mitigate these risks in this paper.

DNBs leverage cloud for speed and efficiency

According to IDC Digital Native Business, Start-Ups and Scale-Ups CIS, the digital native market segment is "an emerging and fast-growing group of organizations, is obviously very tech centric, and spends a significant amount of money on technology as it is the basis of the industry's business model".

Regardless of industry or market, DNBs leverage technology as a differentiator and for greater agility.

By their very nature, DNBs embrace cloud-native design principles in building their technology infrastructure. In fact, DNBs are increasingly spending on cloud-based technologies at an expected 2021–2026 growth rate of 37.3%.



Selected segment growth rate

- Cloud based (SaaS, PaaS, IaaS) CAGR 37.3%
- Noncloud (software and hardware) CAGR 16.7%
- IT services CAGR 11.5%
- Business services CAGR 10.4%

Total market CAGR

20.8%

Source: IDC Press Release, Asia/Pacific Digital-Native Business Tech Spending from 2022-2026 to Grow at a CAGR of 20.8% and Hit US$128.9B in 2026, IDC Forecasts, 19 April 2023

The DNB technology infrastructure is built around a composable architecture of microservices, enabling flexibility, agility, and rapid time to market — essential to keeping up with the fast-growing digital space.

According to the survey, three in four DNBs across the region are deploying cloud technologies as they prioritise efficiency and productivity.

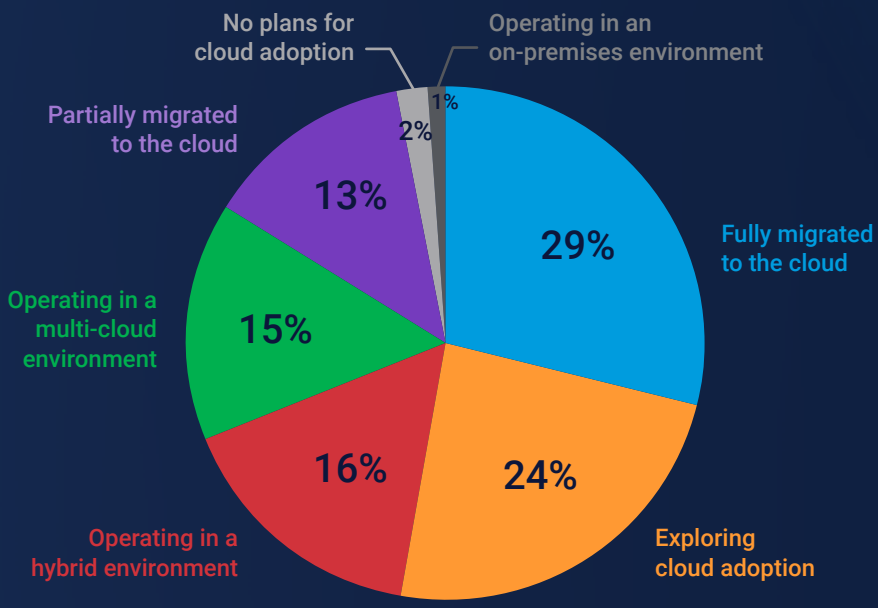
A total of 74% of respondents have either fully migrated to cloud or are adopting cloud technologies.

However, 26% of the respondents either do not have plans for cloud adoption or are still in the exploratory stage, and this is consistent across the region (19% Australia, 20% India, 29% ASEAN).

This reticence is probably due to large incumbent enterprises in highly regulated industries coupled with a long-standing cautionary approach to cloud that continues to be an impediment to cloud adoption.

But there is a thawing happening as DNBs ramp up their cloud investments. This is evidenced by the high growth rate in cloud tech spend.

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



Top business priorities in the next 12 months

Securing life online

The common refrain is how DNBs are proficient in technology. However, this proficiency may be confined to specialist areas.

Although DNBs may be born in the cloud, they may also struggle to leverage the full potential of emerging technology in cloud, data, and artificial intelligence (AI).

We mapped the challenges that respondents encountered with cloud migration against where they are in their cloud journey.

There is a consistent struggle to understand cloud spend among respondents who have fully migrated to cloud and those who are still exploring cloud adoption.

Although most cloud providers are transparent with their pricing, the cost breakdown can be complex. DNBs need to possess the right knowledge and the time to predict and decipher the costs for microservices and multicloud deployments that all scale differently based on various factors. For example, what drives a scalability event — is it end-user demand or inter-process communication?

Top 3 challenges encountered with cloud migration

	Managing security implications	Selecting the right cloud provider	Assessing technical feasibility
Fully migrated to the cloud	45%	53%	57%
Exploring cloud adoption	63%	62%	52%
Operating in a hybrid environment	74%	49%	54%
Operating in a multi-cloud environment	50%	44%	47%
Partially migrated to the cloud	45%	41%	41%

Other challenges:
Understanding cloud speed allocation, prioritising apps to migrate, rightsizing/selecting the best instance, assessing on-prem vs. cloud costs, lack of technical expertise, understanding app dependencies

This has driven DNBs towards cloud providers that offer easy-to-understand pricing without sacrificing performance, reliability, or support.

However, managing security implications remains a consistent challenge, regardless of where DNBs are in their cloud journey — operating in a hybrid environment, operating in a multicloud environment, or having partially migrated to cloud.

In fact, security is currently viewed as the biggest gap in cloud infrastructure among most survey respondents.

Akamai maintains simple, transparent pricing with extremely low egress fees, a generous monthly egress allowance, and tools to maximise data centre and cloud traffic offload.

Together, these represent numerous opportunities to optimise costs for data- and traffic-intensive applications by leveraging Akamai's global footprint.

When choosing a cloud provider, security features outweigh even performance, reputation, scalability, and cost.

Where do you see the biggest gap in your cloud infrastructure's performance or capabilities?

	Security	Network latency	Data storage and retrieval	Compute resources
Fully migrated to the cloud	65%	65%	67%	47%
Exploring cloud adoption	81%	58%	67%	62%
Operating in a hybrid environment	74%	66%	49%	46%
Operating in a multi-cloud environment	84%	66%	66%	63%
Partially migrated to the cloud	69%	62%	62%	24%

Factors when choosing a cloud provider

Tech-first mindset — DNBs' Achilles' heel?

This is where technology may be both a boon and a bane for DNBs.

A majority of respondents cite their complex IT infrastructure as the biggest challenge in enhancing their cybersecurity posture.

Digital natives embrace cloud-native design principles that prize composable microservices and APIs to connect them.

These APIs accelerate technology deployment and speed to market, enabling DNBs to iterate fast and deliver functionalities rapidly.

But that speed and composability come at the cost of complexity when the developers tied to various services do not have the incentive to focus on the DNB's operations.

Security teams and technology will find it a challenge as most security tools do not support hybrid environments and because embedded cloud security tends to focus only on the provider's cloud.

For example, game providers are keen to work with cloud infrastructure providers who are trusted partners rather than vendors as games take years to develop.

Game companies and their developer teams want insight into all aspects of cloud computing, including performance, resource allocations, latency, and throughput, as well as predictable pricing and transparency on billing.

A pay-as-you-go and pay-for-what-you-need distributed cloud computing infrastructure is highly attractive to game providers who like to closely monitor any operating expense not related to directly developing or upgrading their games.

The survey findings highlight that DNBs are faced with an increasingly complex IT infrastructure, which is affecting their organisations' cybersecurity posture.

Biggest challenge in enhancing cybersecurity posture

	Complex IT infrastructure	Local compliance requirements	Lack of skilled personnel	Budget constraints	Rapidly evolving threats
Fully migrated to the cloud	43%	7%	13%	12%	25%
Exploring cloud adoption	37%	6%	10%	27%	21%
Operating in a hybrid environment	49%	3%	9%	23%	17%
Operating in a multi-cloud environment	59%	13%	13%	6%	9%
Partially migrated to the cloud	31%	7%	17%	14%	31%

Balancing risk vs reward

Here's a reality check: Applying consistent security policies across clouds is hard.

Younger DNBs may be excited about the pace that cloud technologies allow them to achieve, but as a business matures, DNBs have to balance risk and reward with each tech innovation. Each innovative tech introduces an additional layer of complexity.

So, how do you balance speed to market and customer adoption versus security, compliance, and governance to avoid a breach or misuse?

This persists as a top challenge in enhancing cybersecurity, regardless of where DNBs are in their cloud journey.

> *Akamai Connected Cloud is an open platform that embraces open-source and multicloud architectures. The architecture has been purpose built to make it easy for developers to leverage the applications and software they want with the services they need to power globally scalable, regionally optimised, low-latency workloads*

Cloud technology itself has shape-shifted from only providing infrastructure to providing a full range of services, including infrastructure management.

Running a cloud-native infrastructure presents concentration risks as well as complex infrastructure challenges.

Here are some considerations to weigh regardless of where you are in your cloud adoption journey:

Adopt a multicloud strategy

Organisations should embrace a multicloud approach to avoid vendor lock-in, enhance flexibility, and optimise cloud service usage.

According to IT leaders surveyed by Forrester Research, the number one requirement for cloud vendors is the ability to deploy and execute from cloud to edge.

Concentrated dependency on a particular vendor can reduce future technology options and allow vendors to exert significant influence over the organisation's technology future.

Leveraging an agnostic, distributed platform will enable digital natives to seamlessly and quickly access raw data and gain insights from the data spread across a multitude of systems.

Review and iterate regularly

Periodically review cloud costs to analyse and optimise cloud spending, identify areas for savings, and optimise resource usage.

Use monitoring data and real-time analytics to identify areas for optimisation, such as resource allocation, cost management, and security improvements.

Regular monitoring and optimisation ensure that you are getting the most business value out of your cloud investment.

Implement cloud governance frameworks

The more applications (and business processes) depend on a particular cloud provider, the greater the potential breadth of impact a cloud service issue has, which may heighten business continuity concerns.

Develop and enforce cloud governance policies to manage cloud resources effectively, ensure compliance, and control costs.

This model should include access control, security measures, cost management, and compliance requirements. A clear governance model helps maintain consistency and best practices across the organisation.

Organisations may also be unable to meet regulatory demands to address concentration risk across different regulatory bodies, which may have different approaches to concentration risk.

Prioritising advanced API security

APIs are central to DNBs when connecting non-cloud, cloud, and multicloud architectures.

They enable DNBs to achieve new levels of connectivity, productivity, and agility by connecting internal applications, accelerating processes with their business partners, and delivering data services to consumers.

In the pursuit of speed and tech-driven innovation, applications and business processes involving APIs are often initiated and deployed faster than security teams can evaluate their posture.

Misconfigurations and vulnerabilities, together with a lack of API security expertise, expose innovative DNBs to potential cyberthreats.

In fact, a separate industry survey of 631 cybersecurity professionals found that one in two developers is spending up to half their time on API refactoring and remediation.

> ***31%*** *of Akamai-protected traffic is API traffic. Akamai provides the tools to maintain consistent controls over your applications and workloads with integrated user experience optimisation capabilities.*

DNBs across Asia unwaveringly place API security as top of mind to ensure sustainable business growth.

Whether they are scaling up in Australia or gaining market share in India and ASEAN, DNBs are prioritising advanced API security as a top cybersecurity investment area ahead of web/application security and anti-phishing technologies.

Rank the following cybersecurity investment areas from most important (top) to least important (bottom)

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

The conditions for API security errors

Rapid deployment of business-critical process using APIs + Lack of visibility into APIs = Misconfigured or vulnerable APIs

Looking at Akamai traffic data, the manufacturing vertical had the highest percentage of API attacks across Asia-Pacific and Japan.

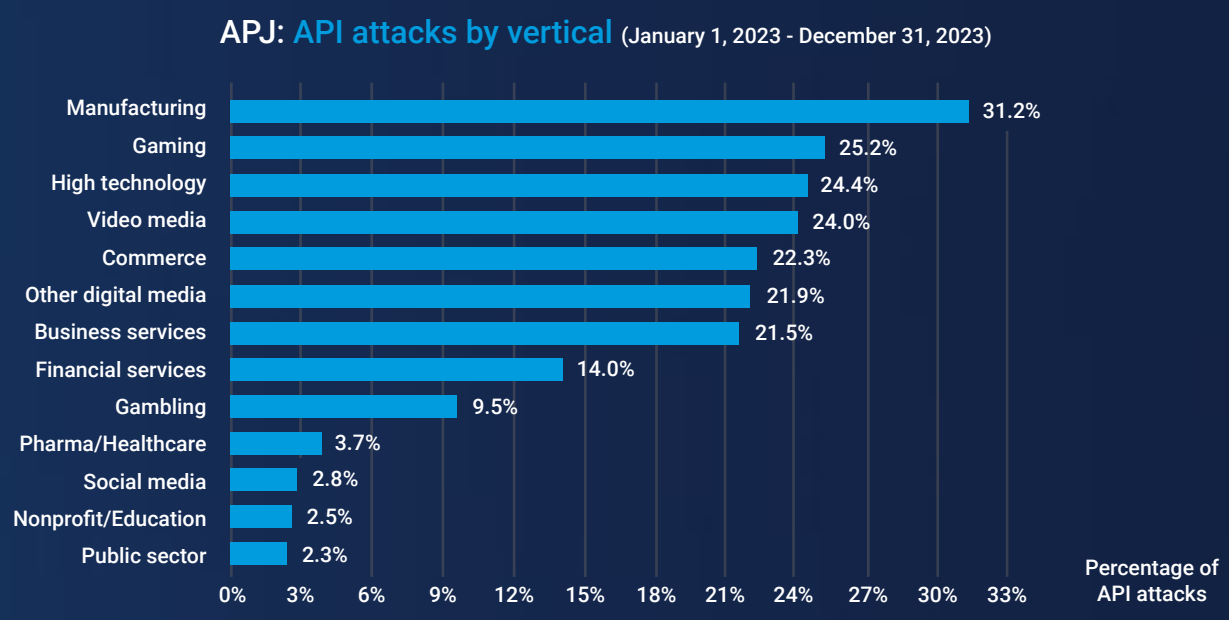
This may be partially due to the increasing connectivity of this critical infrastructure sector via APIs and the potential for supply chain disruption.

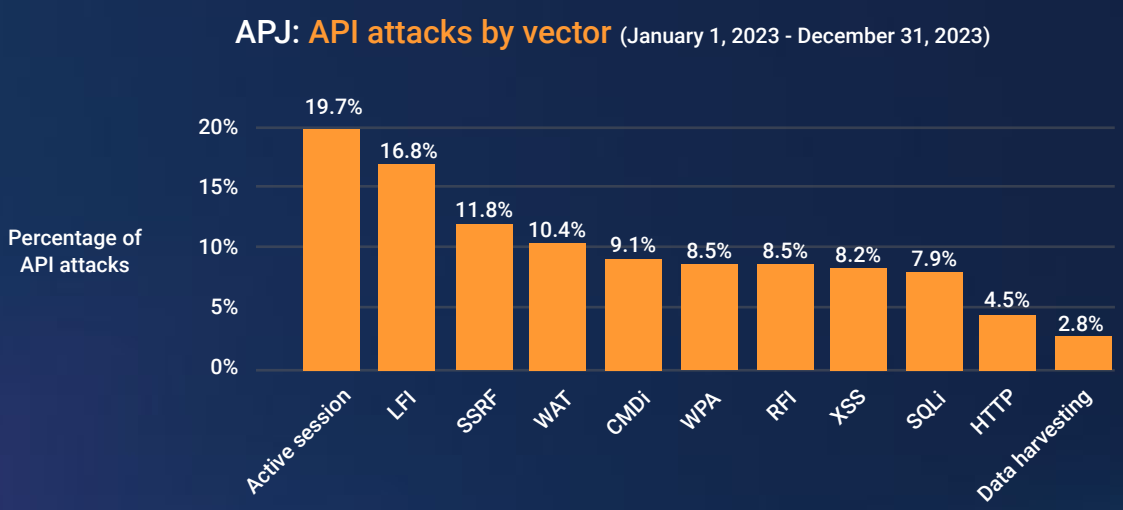
At the same time, digitally driven industries such as gaming, high tech, video media, and commerce are also in the API attacker crosshairs.

The reasons digital natives are most targeted are likely that a significant portion of their business depends on APIs, that they have the most deployed-to-cloud infrastructures, and that they represent the most attractive targets for phishing, account compromise, and ransomware compared to legacy companies and architectures.

Local file inclusion (LFI) remains the top API attack vector, but the 2023 dataset surfaced additional vectors, such as command injection (CMDi) and server-side request forgery (SSRF). These vectors pose significant risks to APIs that are vulnerable, misconfigured, or undocumented.

Bot requests are also an area of concern. During the same 12-month reporting period, 40% of the more than two trillion suspicious bot requests were aimed at APIs.





Critical API security considerations

API vulnerabilities are constantly evolving. Understanding some of the biggest API security risks keeps your organisation ahead of the battle.

Discovery and visibility

Outdated or previous versions of APIs that have not been retired or properly documented expose businesses to increased levels of risk. Examples like shadow APIs exist and operate outside the management scope and can be a point of vulnerability.

Runtime protection

As APIs are executed to actively exchange data, it can be hard for traditional security tools to discern between a legitimate and malicious request by an API. Evasive threats like API logic abuses are known to be difficult to detect because of their ability to blend in with normal API requests.

API testing

API security testing must be baked into every phase of development to improve security without sacrificing velocity. From both cost and remediation perspectives, it is easier to correct issues during an API's development phase than after the API is released into production and actively used.

Unauthenticated resource access

Authentication and authorisation are more complex for machine-to-machine scenarios. A user or system may be able to access API resources without providing any form of authentication, often as a result of flaws in the API implementation or configuration.

Sensitive data in URL

Sensitive data in URLs is often stored in places that may become accessible to attackers, like logs and caches, creating a significant risk of sensitive data leakage and compliance issues.

Permissive cross-origin resource policy

APIs may allow requests to originate from a wider range of origins (such as protocols, domains, and ports) than necessary.

API security–first culture from the start

Nine in ten DNBs surveyed mark API security as a critical or important product feature when evaluating a cloud/security solution provider.

As the pace of technological innovation and third-party connections accelerates, DNBs need support from their vendors to identify potential weak links that can be exploited by cyber adversaries.

API security needs to be baked into every stage of the development process. A lack of an API testing framework and specific API testing tools may contribute to more vulnerable APIs being published, leading to an increase in API security–related incidents. Lack of visibility into API business logic abuse is another factor that leads to API data breaches and fraud.

For example, how does the security team know when an API is being abused while in operation?

What attacks are hitting your organisation's APIs at any point in time?

Security teams may not fully understand the purpose of an API endpoint, for example, and will find it a challenge to know what back-end workloads are interacting with them or what data types are being exchanged. Development teams may also overestimate their ability to fix bugs late in the development cycle.

AI-powered discovery and profiling are important trends in API security, but a security-first stance early in the development process (DevSecOps) helps shrink DNBs' vulnerability early, helping to establish a secure-by-design API development philosophy.

Identifying these advanced API security blindspots from the start can help build a more robust cybersecurity posture.

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

	Critical	Important	Somewhat important	Neutral	Somewhat unimportant
API security	45.60%	45.10%	7.40%	1.90%	0.00%
Customisable cloud security policies	31.20%	53.90%	8.40%	6.50%	0.00%
Edge computing capabilities	29.80%	47.00%	15.80%	6.00%	0.90%
Observability	28.40%	52.10%	11.20%	7.00%	0.90%
Real-time analytics and reporting	45.60%	34.40%	11.20%	7.40%	1.40%
Zero Trust	32.60%	39.10%	14.40%	9.30%	0.90%

Common API security blind spots

Unauthenticated resource access attempt

This is a more urgent derivative of the unauthenticated resource access posture alert described in the previous section where we see specific attempts to access sensitive API resources without the appropriate authentication. Even if the observed attempts are unsuccessful, these scenarios suggest an active attempt to find and exploit API vulnerabilities, which may eventually be successful without prompt intervention.

Abnormal JSON property

API activity with unusual JSON payloads, such as unexpected data types, abnormal size, or excessive complexity, may indicate an active attempt to exploit a vulnerable API. This activity may indicate an attempt to perform a variety of malicious actions, such as injection attacks, denial of service, data exfiltration, or exploitation of API logic flaws.

Path parameter fuzzing attempt

Path parameter fuzzing is another example of deliberately sending unexpected or malformed data as a part of API requests, with a focus on the parts of the URL that RESTful APIs use to specify certain resources or operations. It's another technique that attackers use to perform reconnaissance to discover potentially vulnerable APIs that can be targeted with data exfiltration or service disruption attempts.

Impossible time travel

When analysing API activity, there are scenarios in which the timestamps, geolocation, or sequence of API calls are illogical, which suggests that attackers are attempting to manipulate them in some way. Additionally, this type of behaviour may represent several possible threats such as data manipulation as part of fraudulent activity.

Data scraping

Data scraping refers to the automated extraction of data from an API in a manner and volume that do not align with the intended use and terms of service for the API. Attackers often collect this data slowly to avoid detection and steal intellectual property, gather sensitive customer data, or gain some kind of profit. When it goes undiscovered within APIs, low and slow data scraping is a potentially massive data breach attack.

A modern API security approach

Modern APIs are the connective tissue, enabling microservices, multicloud, seamless integration, and rapid expansion. They are the soft underbelly of any application or workload and must be architected, developed, and deployed correctly to optimise business outcomes.

However, organisations tend to apply the same security measures even though modern API transactions tend to have unique characteristics, such as high-frequency transactions.

1 Implement automated API discovery

Ensure that the APIs you provide and use are properly identified to protect against API-related security breaches, unknown dependencies, and unexpected inconsistencies. Native integrations to API data sources will help reduce both complexity and operational overhead.

2 Managing the posture of APIs

Evaluating API security involves detecting any misconfigurations, performing a penetration test, or using automated assessment tools that proactively scan for configuration issues such as APIs exposing sensitive data in URLs. Automated responses ensure that a relevant party such as the API development team can be called upon to fix the issue as part of the response workflow.

3 API runtime protection

This involves detecting patterns that indicate malicious activity. An anomaly detection engine, trained on datasets of similar attacks, should be able to identify threats and alert concerned parties. Response workflows can be triggered to raise remediation tickets or block potential threats upon detection of abnormal API traffic.

4 Proactive security testing

API security testing through dynamic scanning and fuzzing can uncover technical vulnerabilities that may not be detected as misconfigurations during the initial assessment.

As your API security matures, security testing should be more tightly integrated into the API development lifecycle, with vulnerabilities addressed as they are discovered — before reaching production. This means cross-functional alignment between security and development teams.

5 API security ecosystem

Having a rich and robust technology ecosystem where the API security solution is able to natively integrate and interoperate with third-party technologies cuts costs and implementation time. It also gives wider API traffic visibility from data sources, quicker threat response via automated workflows, and overall better API security posture.

Australia/New Zealand: From start up to scale up

Analyst reports point to weak domestic demand and soft labour demand in Australia/New Zealand (ANZ) in the coming years.

Customers are already feeling the financial pressure with slow wage growth and persistent inflation.

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

There has also been a mindset shift as cloud tech now becomes a business essential. A total of 97% of respondents have either embraced cloud or are exploring cloud adoption.

ANZ organisations may be 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

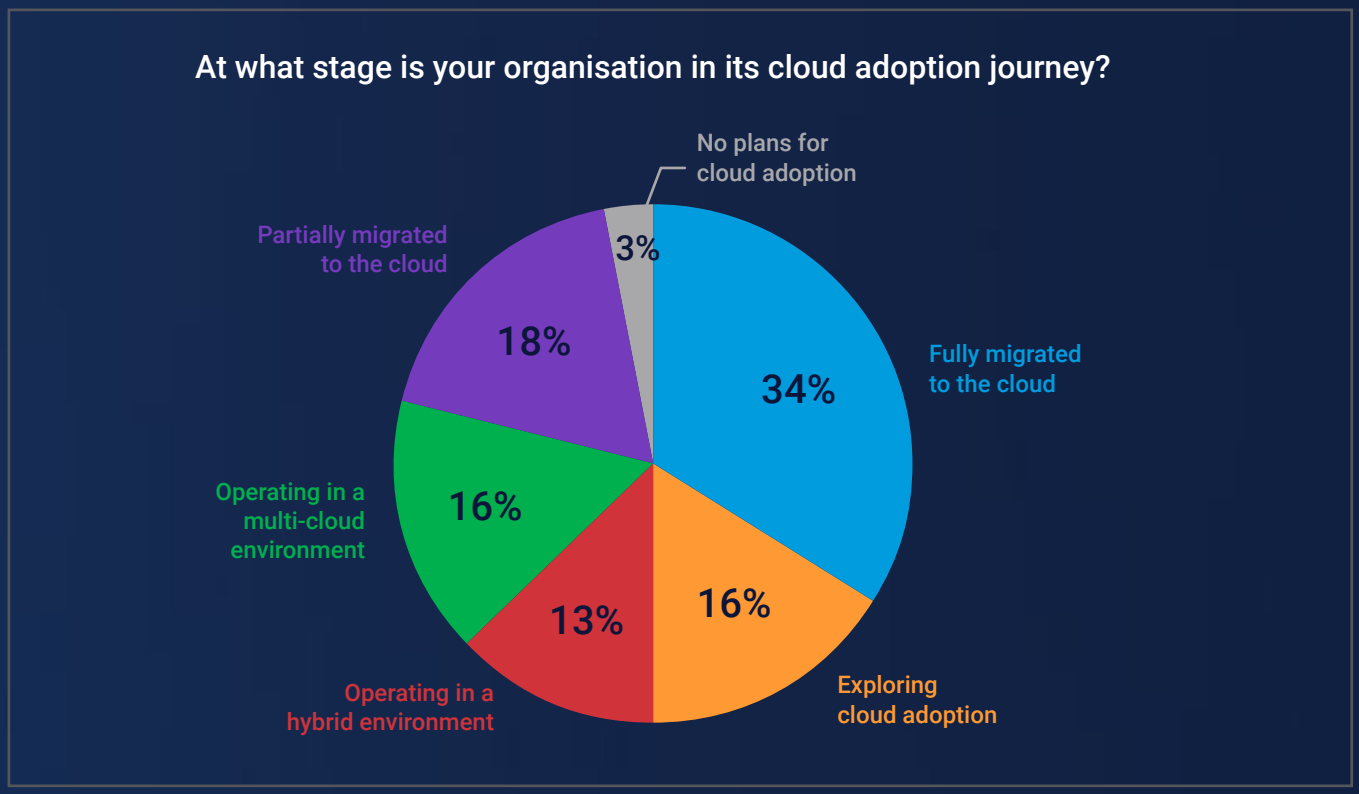
For example, ANZ's public cloud adoption has moved beyond discrete software as a service–based solutions for infrastructure replacement, like disaster recovery, to advanced use cases driving organisation-wide digital transformation and innovation.

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

The public sector is also a dominant force propelling cloud adoption in both Australia and New Zealand, with New Zealand 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).

Being further along the digital adoption curve means that ANZ organisations may have legacy applications that are not architected for the cloud, not containerized, or not microservices based, meaning they 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 security implications and the lack of technical expertise.

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 microservices and multicloud deployments, which all scale differently based on various factors.

Cloud cost management solutions such as FinOps introduce financial accountability to the cloud's variable spend model. Users are held accountable for spend decisions with visibility into the organisation's cloud usage and productivity optimisation opportunities.

What are the top challenges that you encountered with cloud migration?

Strategies to avoid vendor lock-in

Third-party tools to optimise cloud costs

ANZ's IT leaders are leveraging third-party tools, managed services, and contract negotiations with higher amounts of committed spend or larger committed growth rates in exchange for discounts.

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

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

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.*

Richer customer experience means more sensitive data

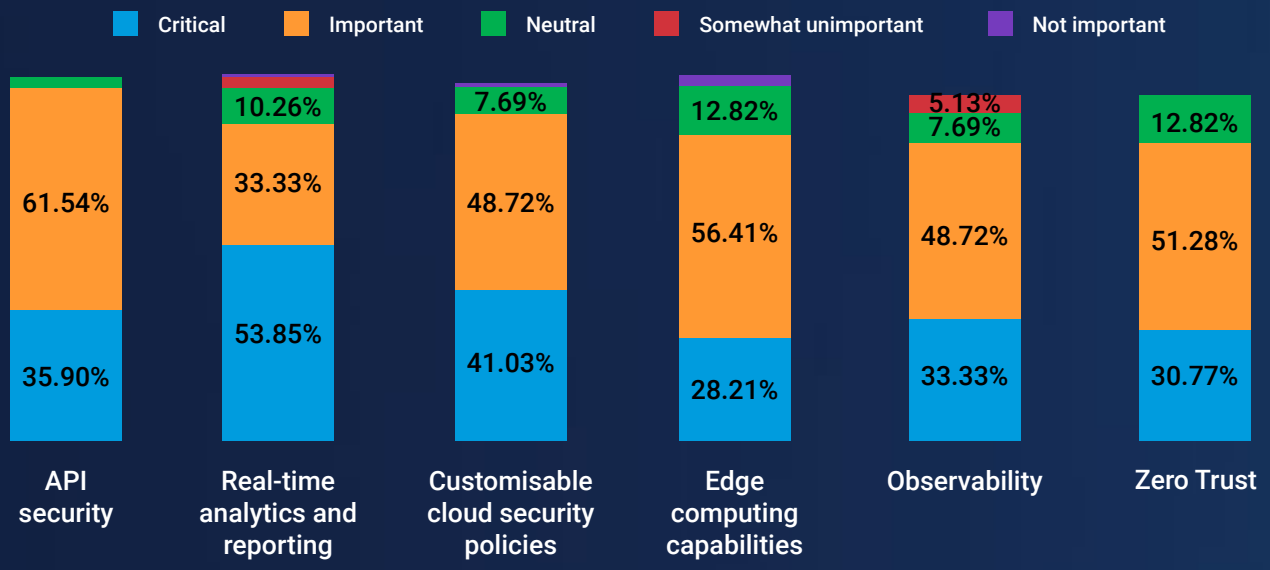
With a relatively mature customer digital adoption, ANZ businesses want the ability to ingest, process, analyse, and act on real-time data to provide an optimal user experience.

A total of 87% of ANZ respondents cite real-time analytics and reporting as a critical/important product feature in their evaluations of a cloud/security solution provider.

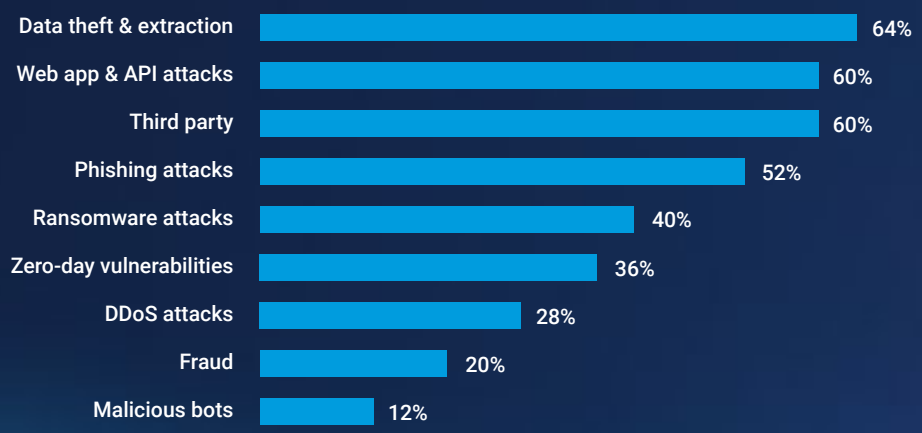
At the same time, the pursuit of richer customer experiences among ANZ digital natives also risks exposing them to cyberattacks targeting rich personal and financial data.

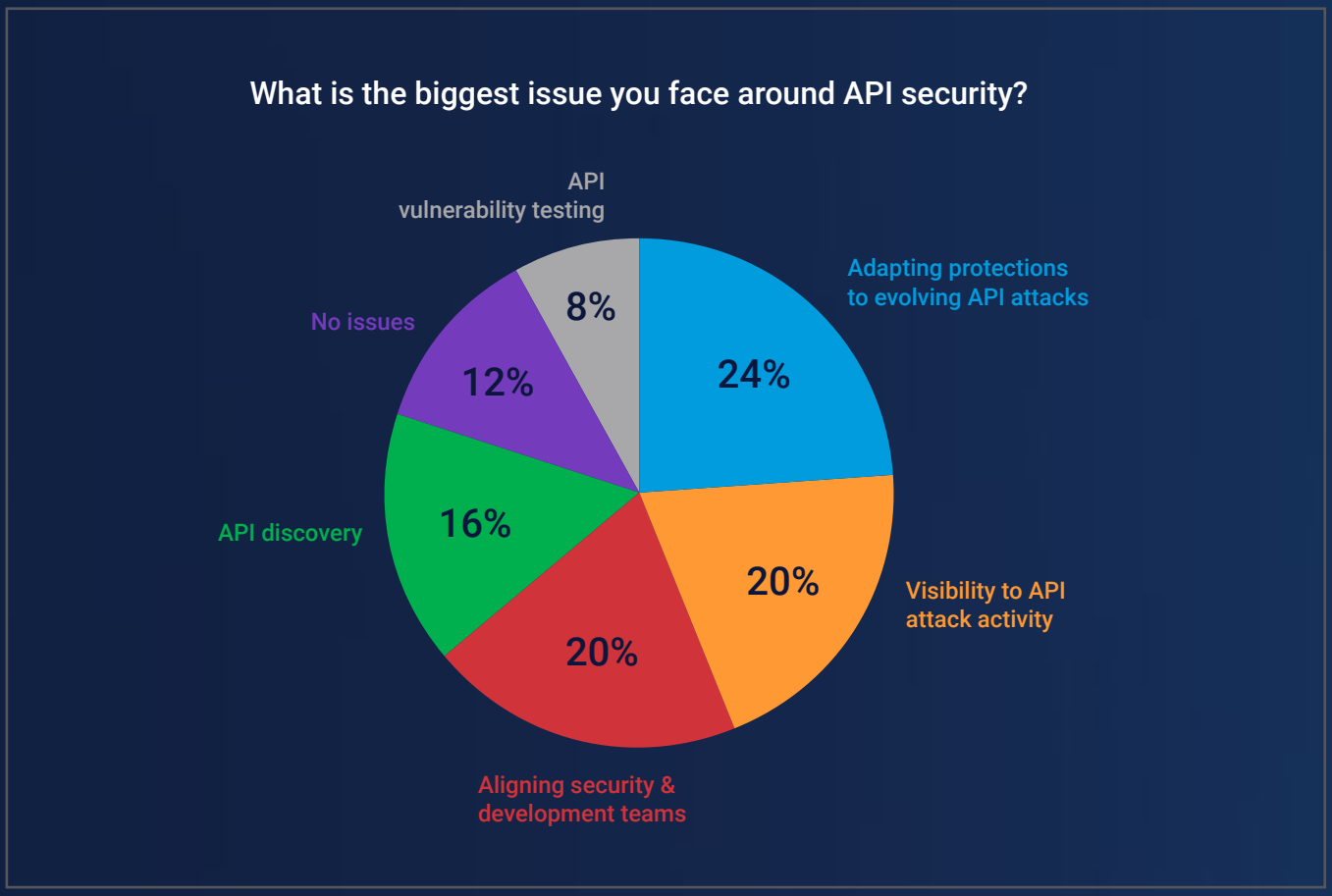
Web application and API attacks together with data theft and extraction were among the top cyberthreats of concern for IT leaders in Australia, according to Akamai's Cybersecurity in Financial Services report.

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 also a security dimension, as ANZ IT leaders feel that the biggest issues they face around API security are gaining visibility into 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 operate in their environment without their knowledge.

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

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

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).

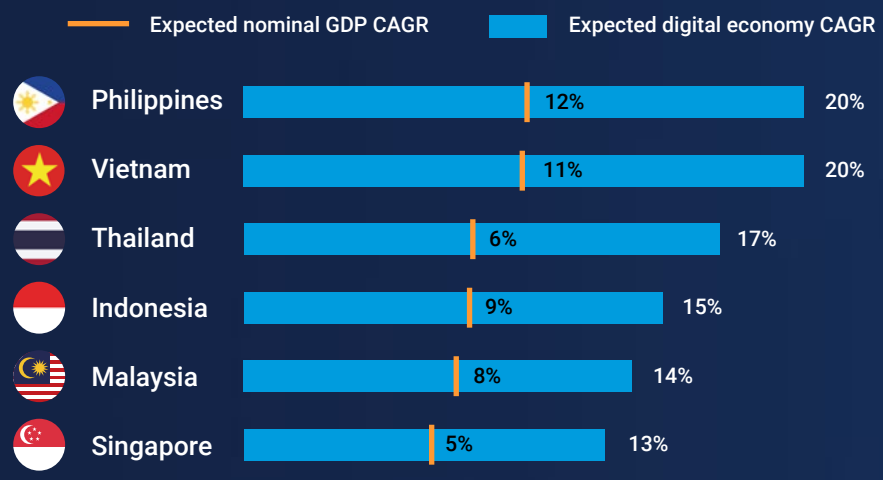
Digitally native and connected millennials and Gen Z are expected to account for 75% of ASEAN consumers and 70% of Indonesian consumers by 2030 (Source: World Economic Forum).

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

While ASEAN consumers are rapidly embracing the digital life, the region's infrastructure still needs to keep up. The digitally savvy younger generation has high expectations for service uptime and low latency.

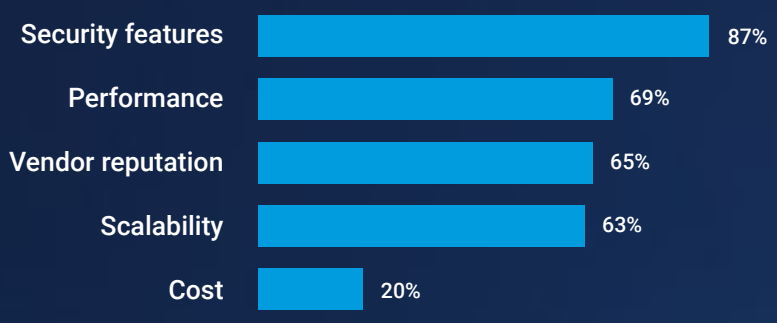
It is thus to be expected that performance and vendor reputation rank highly, at 69% and 65%, respectively, for vendor selection among the ASEAN respondents.

Digital economy GMV growth vs. GDP growth (2023-2025)



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

Factors affecting cloud vendor selection



At the same time, network latency is a persistent issue for DNBs in ASEAN.

The region still needs to ensure high-speed and reliable internet connectivity and the widespread availability of electricity in urban and rural areas. Uneven connectivity still occurs across geographically disparate countries like Indonesia with its 17,508 islands (unofficial sources put the figure closer to 25,000 islands!).

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

Governments across the region have been actively investing in connectivity to bolster continued growth.

Indonesia recently completed the Palapa Ring project, bringing 4G internet connectivity to the most outlying regions, with more than 35,000 km of land and sea fibre-optic cables across the country.

> *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.

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.

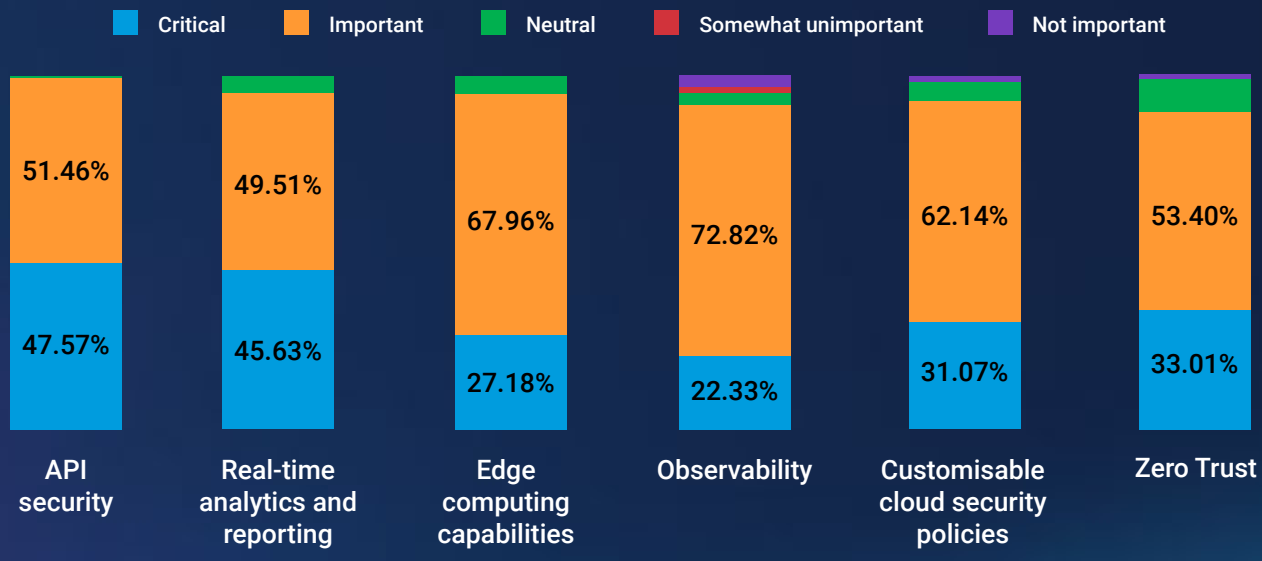
Visibility is a critical aspect of API security. Once blind spots like shadow APIs or rogue APIs are illuminated, security teams can start to address vulnerabilities that they were previously unaware of.

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 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.

Phishing is not going to go away.

The rise of generative AI will make phishing attempts more convincing and open up 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.

Detected and blocked financial phishing in Southeast Asia in 2023

Country	Number of financial phishing
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 (top) to least important (bottom)

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

India: “I” for innovation

India has been the epicentre of innovation and DNBs for over a decade and the leading source for cloud-native architectures and experimentation.

For DNBs in India, the focus has been on growth and innovation, with the highest AI integration within the cloud infrastructure (98%) in the region and almost all DNBs either already in cloud or exploring cloud adoption.

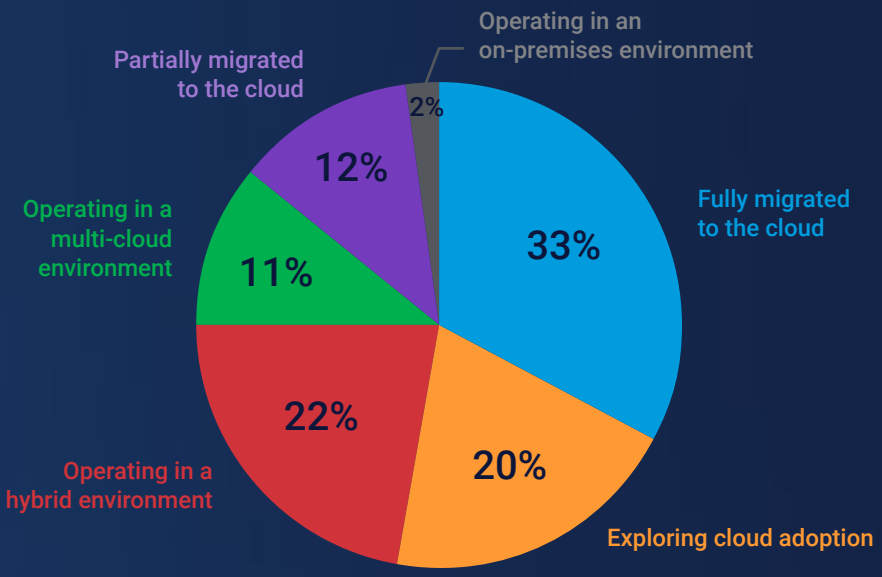
But as DNBs in India mature, they are starting to look at sustainable growth by focusing on security and cost optimisation and by reviewing vendor selection closely.

The customers of early DNBs in India are often technology companies themselves.

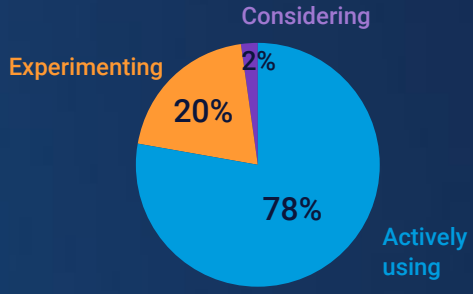
Powered by APIs, India’s DNBs have been able to lend tech support and expertise to companies globally without directly accessing the customers’ data. India’s DNBs invested in expertise, APIs, and custom-built systems early on.

With such a deep heritage in technological excellence, India’s digital natives place a higher priority on vendor performance than do their regional peers (second in ASEAN and fourth in ANZ).

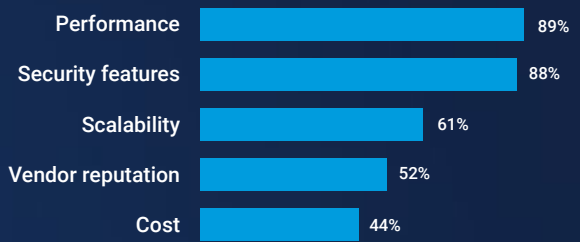
At what stage is your organisation in its cloud adoption journey?



Current level of integration of AI technologies within cloud infrastructure



Factors affecting cloud vendor selection



“I” is also for in-house expertise

What also stands out for India’s digital natives is the do-it-yourself approach to cloud cost management compared to its regional counterparts.

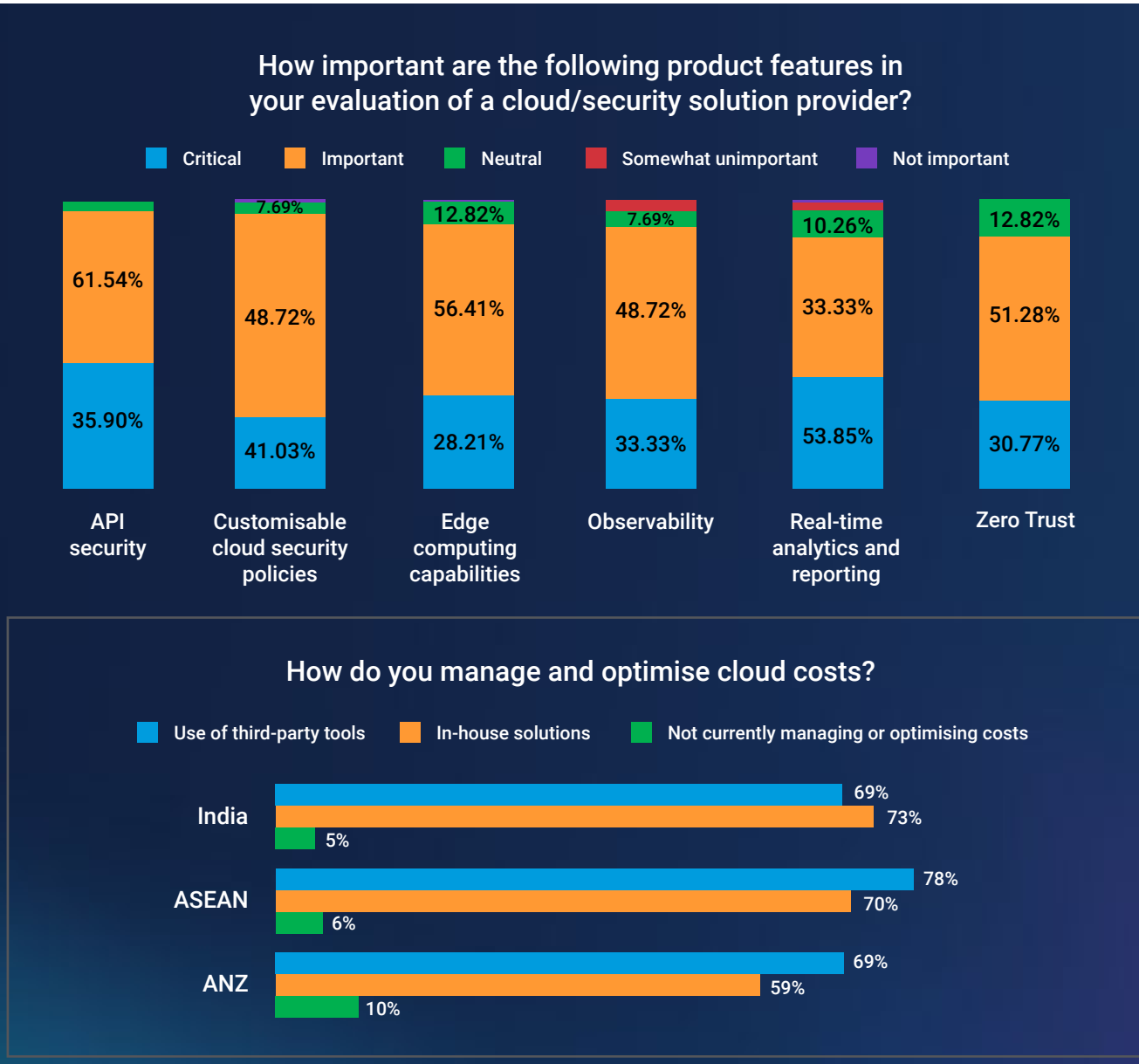
In India, a total of 73% of respondents report using in-house solutions to manage and optimise cloud costs, in contrast with respondents in ASEAN (78%) and ANZ (69%), who prefer to use third-party tools.

The ANZ respondents’ preference for third-party tools may be due to the local IT skills shortage.

For example, there is a need for 5,000 cybersecurity workers annually in ANZ, but the local education system is only expected to produce around 2,000 workers with cybersecurity expertise by 2026.

In contrast, there is an abundance of skilled talent in India, with its historical strength as the world’s technology services hub.

Over 1,600 global capability centres (GCCs) in India currently provide tech support to the organisations globally, and that number is set to increase by 2030, with around 2,500 GCCs employing over 4.5 million people and generating US$100 billion in revenue.



DIY exposes India's DNBs to vulnerabilities

The DIY approach of India's digital business in managing their technology infrastructure may expose them to vulnerabilities as they scale and mature organisationally.

Integrating different systems with multiple APIs already increases potential attack surface. This issue is exacerbated further for organisations born in the cloud and fully running services online.

Three in five respondents in India cite managing security implications around cloud infrastructure and migration as a top issue. In fact, three in four respondents cite security as the biggest gap in their organisation's cloud infrastructure.

India's DNBs need to see both sides of the lens to see their organisations' vulnerabilities and potential attack scenarios. The cyberthreat landscape is fast evolving, with new attack methods and tools increasing in sophistication.

India's DNBs may need to remove the shackles of technological self-sufficiency by partnering with third parties who have specialist skills and leverage the efficiencies that emerging technologies can offer.

As it is, a sizable proportion (41%) of the survey respondents cite the complex IT infrastructure as their biggest challenge in enhancing their organisations' cybersecurity posture. In comparison, 36% of ANZ's respondents cite a complex IT infrastructure as a challenge.

Attempting to manage cybersecurity in house without the help of 24/7/365 experts may no longer be a viable option, especially for a fast-growing market like India that also happens to be one of the top cyberattack targets in the region.

This will be the core piece in India's technological infrastructure jigsaw puzzle.

> *Akamai's distributed cloud platform offers developers control over where to deploy and scale compute resources. Developers have the power and flexibility to define where data is captured, processed, and managed.*

Stronger together

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.

However, it would be naïve to paint all digital natives with a broad brush stroke.

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 are looking to balance security and privacy with the user experience.

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. The survey 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