Focus on India

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 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 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.

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 India.

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.

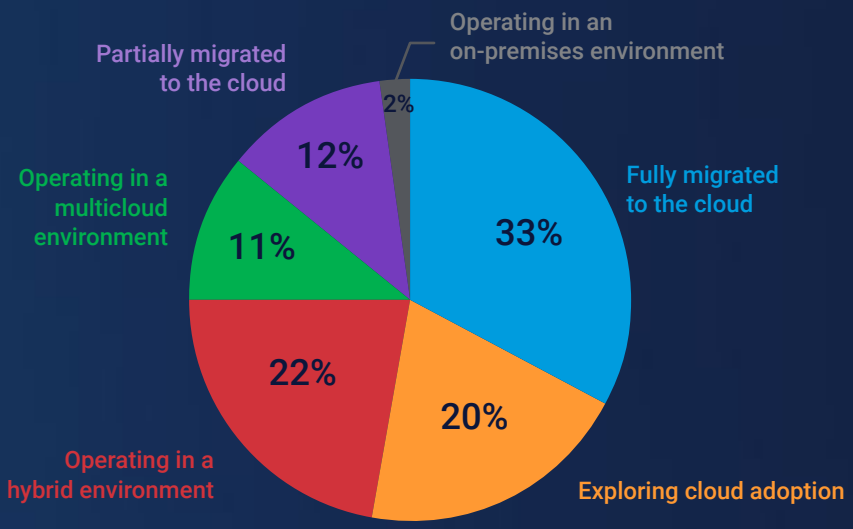
The customers of early DNBs in India are often technology companies themselves.

Powered by APIs, India’s DNBs have been able to lend tech support and expertise to companies globally without directly accessing the customers’ data.

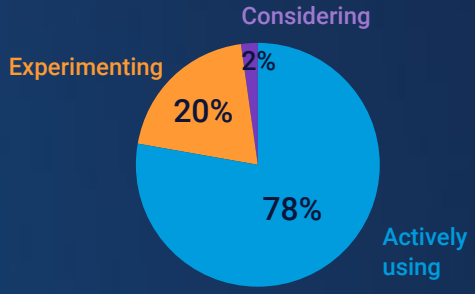
India’s DNBs invested in expertise, APIs, and custom-built systems early on.

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).

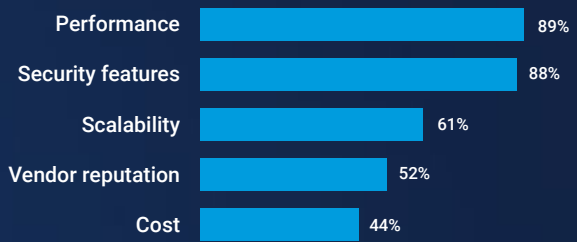
At what stage is your organisation in its cloud adoption journey?



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.

> ***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.***

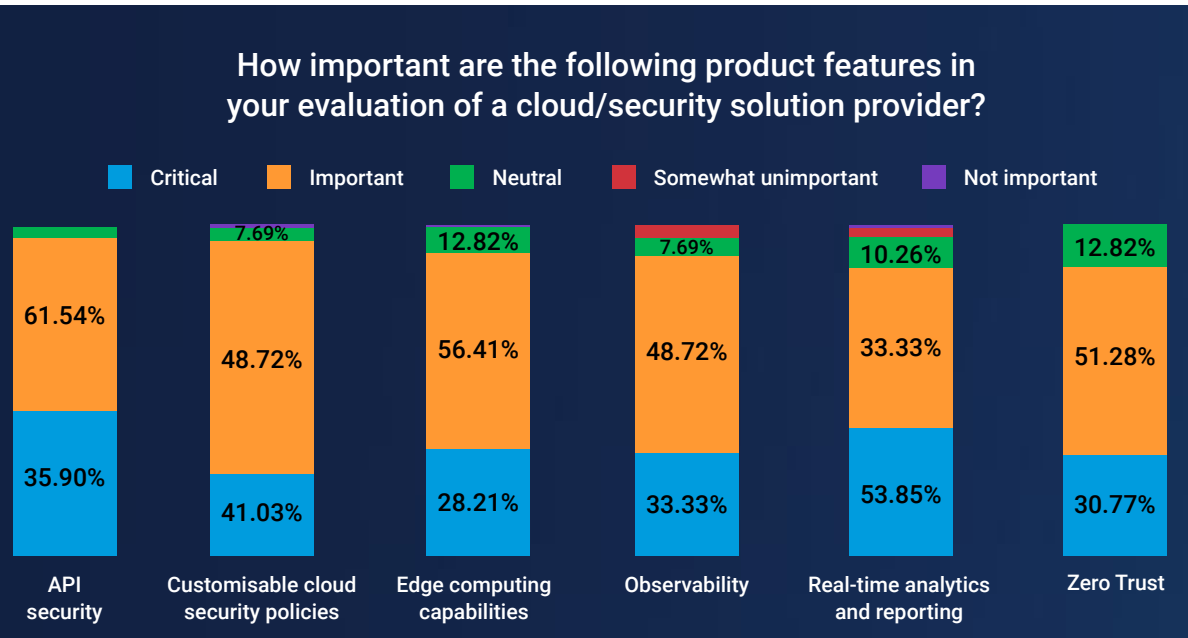
In India, a total of 73% of respondents report using in-house solutions to manage and optimise cloud costs, in contrast with respondents in ASEAN (78%) and ANZ (69%), who prefer to use third-party tools.

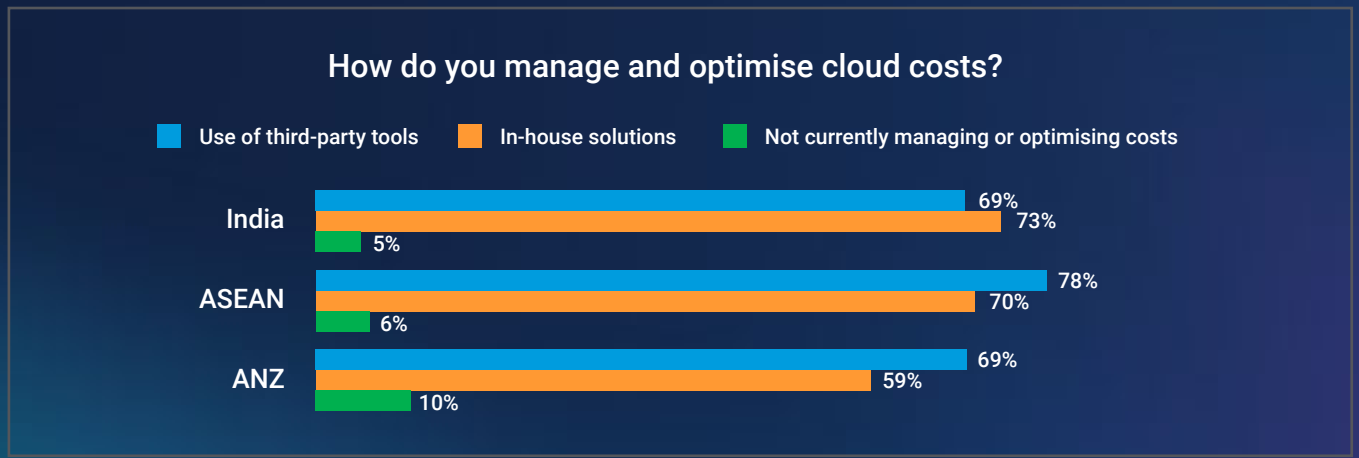
The ANZ respondents’ preference for third-party tools may be due to the local IT skills shortage.

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 sizeable proportion (41%) of India's 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.

B2B APIs — potential blind spot

India's DNB respondents ranked advanced API security as a top cybersecurity investment area ahead of anti-phishing technologies.

API security was also marked as a critical/important feature when evaluating a cloud/security solution provider for 97% of India's respondents.

In a digital-driven ecosystem, APIs enable the seamless integration of disparate parts — serving as conduits for data exchange and communication among applications.

Important cybersecurity investment areas by ranking

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

As a result, APIs are prime targets for cyber adversaries who are seeking to exploit vulnerabilities and gain unauthorised access to sensitive financial information.

Unfortunately, first-generation API security products have repeated the mistakes of the past in this area.

There's a reason for this: Unlike traditional endpoint and application use, API use is not limited by the constraints of human involvement. Data volume for most types of activity grows according to human factors, such as employee expansion or the introduction of new customer-facing applications.

API activity, in contrast, is primarily machine-to-machine communication. Therefore, its growth isn't constrained by human involvement, and it can spike dramatically for both legitimate and malicious reasons.

While B2C API security is now relatively well understood, many security teams overlook the central role that B2B APIs now play in their organisation — and the potentially devastating risks that they expose.

When business partners integrate their key operational functions through APIs, that integration creates a complex web of interconnectivity.

Many of these API-based connection points provide direct visibility and access to core business functions. This may be perfectly fine when the functionality and data is limited to the intended use by trusted partners. But in the hands of a rogue partner or external threat actor, this level of API access can be exploited in ways that could have devastating business impacts.

Because B2B APIs are authenticated, and typically serve a smaller number of API consumers than B2C APIs, it is easy for API and security teams to be lulled into a false sense of security. Many organisations can underestimate their impact on the business.

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.

Case Study: India's online grocer scales up

India's leading omnichannel grocery platform, FreshToHome, aims to provide a one-stop shop for natural and organic foods to customers in India and the Middle East.

Founded in 2015 with just eight employees, FreshToHome has transformed into a trusted omnichannel grocery platform with a workforce of 5,000.

The company relies heavily on technology, including AI and the Internet of Things (IoT), to promptly transport fish and meat directly from fishermen and farmers to its warehouses and distribution hubs.

Operating in 160 cities, including 154 in India and others in the Middle East, FreshToHome has expanded its offerings to include poultry, mutton, vegetables, and dairy. The company also ventured into omnichannel retail through physical stores.

As the company grew, it called upon Akamai to ensure cost-effective, reliable operations.

The company leverages patented AI-based technology known as the Commodities Exchange, enabling fishermen and farmers to electronically auction their products to FreshToHome.

On the back end, an intelligent system predicts product demand and determines the optimal price point. Each distribution hub operates its own software and Internet of Things (IoT) devices, all interconnected with the company's central network.

Additionally, over 2 million customers make purchases via FreshToHome's app every month.

As a rapidly growing business in which inventory plays a crucial role, FreshToHome needed the right cloud computing platform to enable uninterrupted operations.

FreshToHome needed a flexible cloud computing platform that would enable uninterrupted operations and support continued growth across numerous locations. The company, which has experienced nearly fourfold growth in the past decade, decided on Akamai to power its cloud environment.

The Akamai platform proved to be highly cost-effective, as transparent pricing eliminated hidden fees based on usage. This allowed FreshToHome to precisely know the company's expenses when deploying multiple instances.

Saurabh Odhyan, Consumer CTO of FreshToHome, said, "Without the agnostic, distributed Akamai platform, it might not have been possible to seamlessly and quickly access raw data and gain insights from the data spread across our proprietary systems."

Conclusion

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