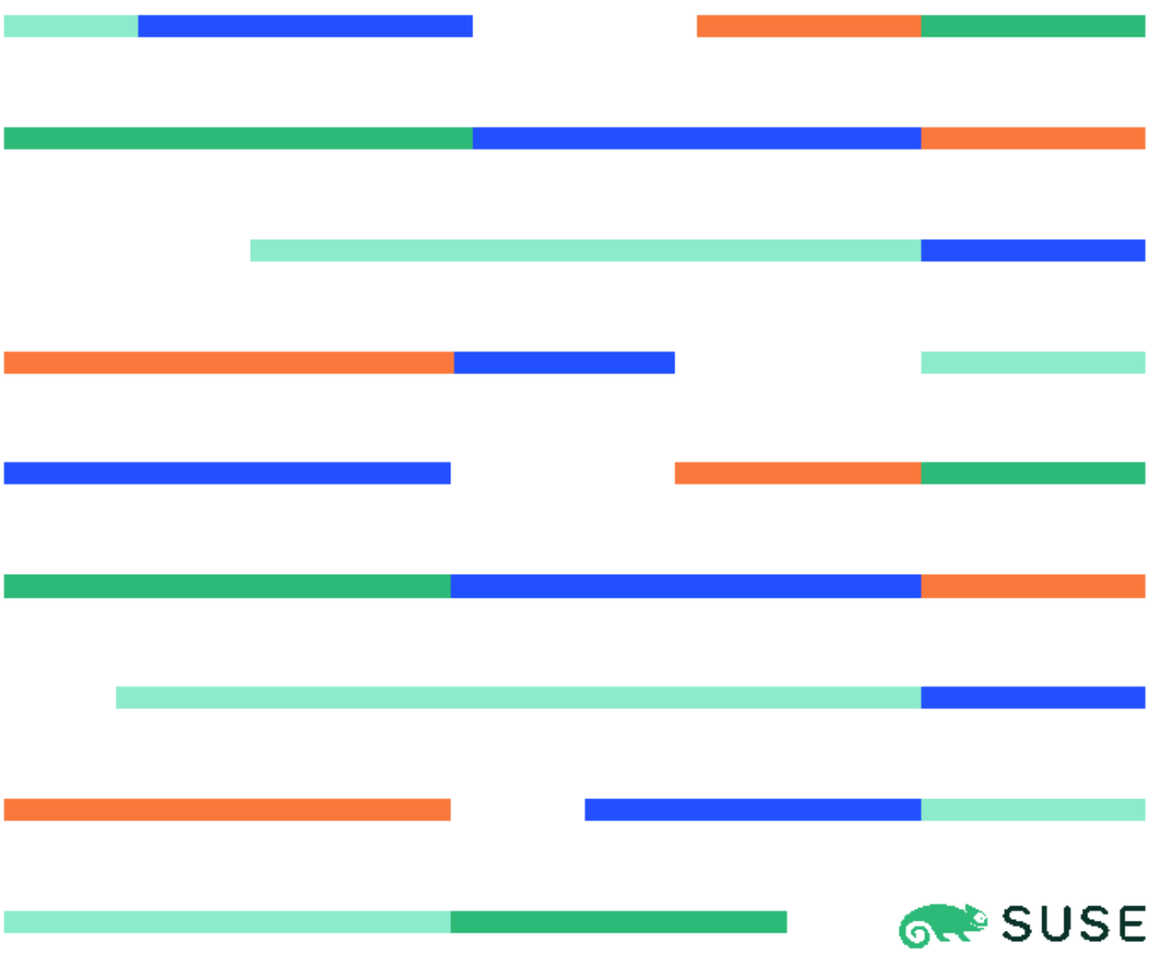
Securing the cloud

2024 APAC Edition

An Asia-Pacific industry trend report on cloud security challenges in the era of AI



SUSE

Sections of the report

Executive summary 3
Key findings in APAC 4
GenAI security 5
Cloud adoption 6
Incidents and concerns 7
Security practices and budget 8
Supply chain security 10
Methodology 11

Executive summary

At SUSE, we recognise that every business around the world is on a journey of digital transformation, and that transformation is enhanced and accelerated by open source software. When we first launched the 'Securing the cloud' trend report in 2023, we investigated how IT teams in the US, UK, and Europe manage and think about cloud security. This year, on the cusp of SUSECON China, we have launched an independent trend report for APAC – a region that so often is at the forefront of global tech innovation.

Understanding how IT decision makers in this region think about some of the most critical tech developments provides invaluable insights into the unique challenges and opportunities they face.

In this trend report, we are also focusing on two major themes that have a profound impact on cloud security – Gen AI and Edge computing. This report considers how the widespread use of increasingly complex cloud environments poses significant challenges, ranging from edge security to AI-powered cyberattacks, and examines how professionals in the APAC region are rising to face these challenges.

The findings of this report indicate significant differences in terms of priorities and concerns between different APAC countries. IT leaders looking to adopt cloud and cloud native technologies are up against several security challenges across the region, with ransomware attacks, GenAI privacy, data security, and AI-powered cyberattacks seen as significant risks.

GenAI has rapidly emerged as a key threat, especially in Indonesia, while Japanese stakeholders show the least concern.

On average, **84% of APAC IT professionals agree that their teams would migrate more workloads to the cloud and to the edge if they knew their data couldn't be tampered with.** There is much higher willingness in China (97%), Indonesia (94%), India (93%), and Singapore (90%) to agree with this statement. On the other hand, Japan stands out as a clear outlier in the region, with only 53% agreeing with this sentiment. .

Additionally**, a majority of IT leaders in APAC (62%) have experienced an edge security event in the past year**.

Security practices across APAC include automation, DoS/DDoS protection, and cloud solutions, with divergences in preferences and implementations. A notable portion of respondents in Japan and Australia report having no current cloud security practices.

Supply chain security remains critical, with an emphasis on in-house auditing and Software Bill of Materials (SBOM) quality. The report underscores the importance of addressing security gaps and regulatory compliance to advance cloud and edge technology adoption.

SUSE is exceptionally well-prepared to support businesses which are choosing open source and looking to transform with the cloud while remaining secure in times of GenAI and Edge computing. Cutting-edge companies are already entrusting SUSE with their mission critical needs.

Key findings in APAC

57%	of IT decision makers are concerned about privacy and data security in Gen AI cloud security
64%	of teams have confirmed a cloud security incident over the last 12 months
62%	of IT decision makers have experienced at least one edge security incident over the past year
27%	of the work of those surveyed is in the cloud
84%	of IT professionals in APAC would move more workloads to the cloud or edge if they knew it could not be tampered with
33%	of IT decision makers intend to review their own software supply chain to increase security
84%	of IT decision makers consider migrating more workloads in the cloud or to the edge if they could guarantee data safety
34%	of respondents point to ransomware attacks as their top security concern

GenAI security

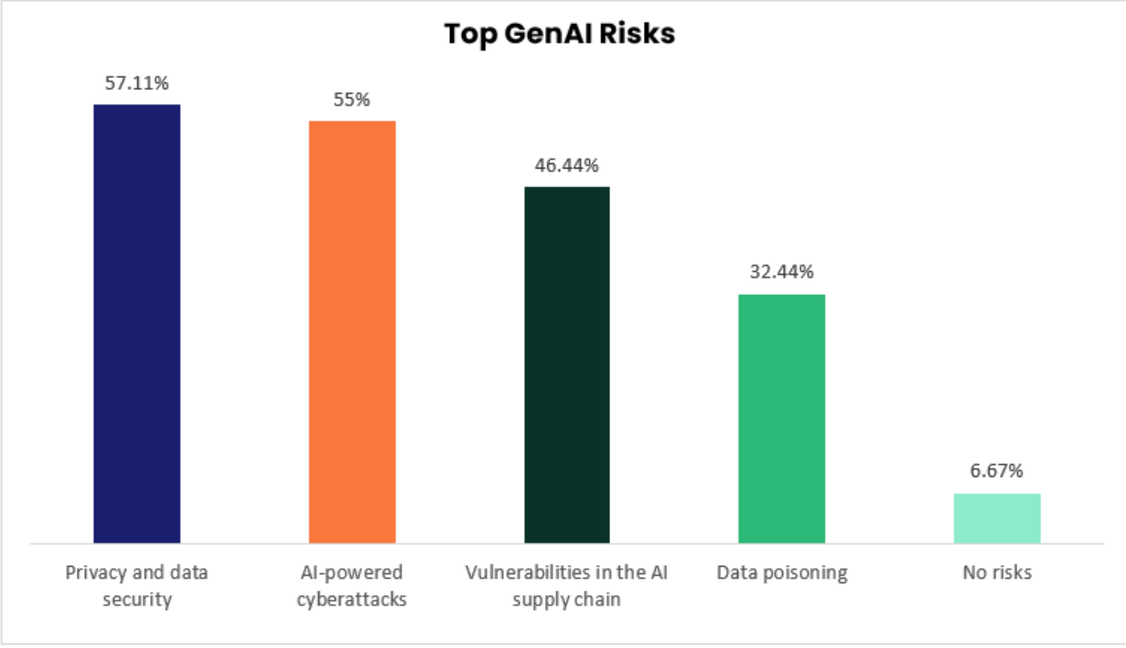
Generative AI revealed as a key security concern among IT decision makers across APAC countries, with threats perceived most strongly by Indonesian stakeholders and least strongly by Japanese stakeholders.

Privacy and data security (57%) and AI-powered cyberattacks (55%) are the top concerns in generative AI cloud security, with only 7% of IT decision makers perceiving no related security risks.

Japanese respondents showed the least concern, with 25% believing there are no GenAI-related security risks. Overall, markets diverged in their perceptions of the strongest risks.

Privacy and data security were the biggest risks in Indonesia (79%), Singapore (66%), China (62%), South Korea (55%), and Australia (52%), whereas AI-powered cyberattacks were the primary concern in India (63%) and Japan (39%). Vulnerabilities in the AI supply chain were also seen as a significant threat across the region, especially in China (59%), Singapore (56%), and India (53%).

Age matters: while very few respondents in the 18-54 age group did not believe there to be any risks (4%), that number was more than double for respondents older than 55 with 10% of respondents, suggesting both more awareness and more engagement with the topic from younger IT professionals.



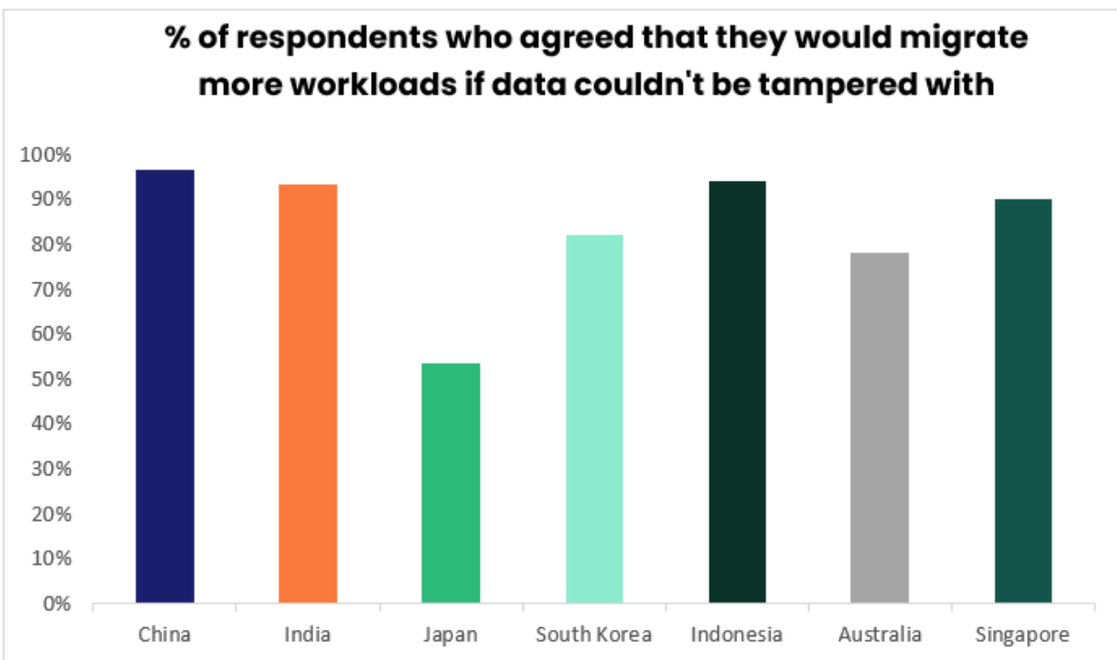
Cloud adoption

Japan is a clear outlier in a region that is overwhelmingly willing to migrate more workloads to the cloud and to the edge, if data safety could be guaranteed.

On average, those surveyed say a quarter (26.7%) of their work is in the cloud – which is slightly lower than in the US / Europe (33.1%). However, there are large divergences among the APAC markets, with IT decision makers from China having both the highest average percentage of workloads in the cloud (37.1%) and the highest median (45.5%). India (30.6%) has the second highest average percentage of workloads in the cloud, followed by Singapore (28.9%). Japan (16.5%) and South Korea (19.7%) have the lowest average of workloads in the cloud. Interestingly, while Australia is mid-field with an average of 27.2% of workloads in the cloud, it has the highest proportion of respondents that reported having over 50% of workloads in the cloud, with 21% (followed by China with 17%).

Overall, APAC IT decision makers are very willing to migrate more workloads to the cloud and to the edge if data safety could be guaranteed, with an average of 84% agreeing with the sentiment. Among Chief Executives, the percentage is even higher, with 97% stating they would be willing to.

Respondents from China (97%), Indonesia (94%), India (93%), and Singapore (90%) were strongest in agreement with the statement, while Japan (53%) proved a clear outlier in the region – indicating larger barriers to cloud adoption in the market.



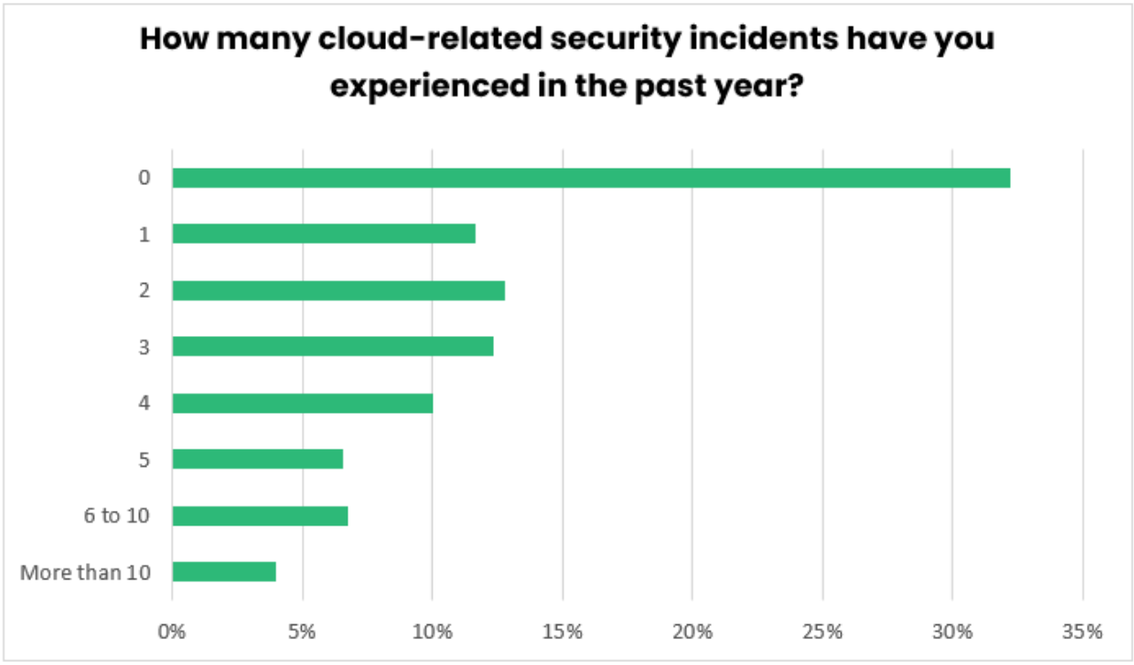
Incidents and concerns

On average, APAC IT decision makers experience at least two cloud-related security incidents annually. Ransomware attacks are the biggest concern – reflecting a trend in other global markets. A third of respondents did not experience any cloud-related security incidents.

APAC IT decision makers report an average of 2.6 cloud-related security incidents in the past year, with India (4.4) and Indonesia (3.8) being the most affected, and Australia (1.2) and Japan (1.8) the least.

Ransomware attacks are the top cloud security concern (34%), reflecting a similar trend in the US and Europe (38%). This is followed by attacks on running services using unknown vulnerabilities (zero-days) at 27%, and visibility controls to sensitive data being accessed in the Cloud and monitoring and alerts on malicious activities behaviours (both 23%).

Again, concerns around different security issues vary considerably by market. Concerns around ransomware attacks are considerably higher in South Korea (48% of respondents identifying it as one of their biggest security concerns) and Australia (44%) compared to only 20% in China.



Security practices and budget

The majority of respondents have experienced at least one edge security incident in the last 12 months – with strong divergences across APAC markets.

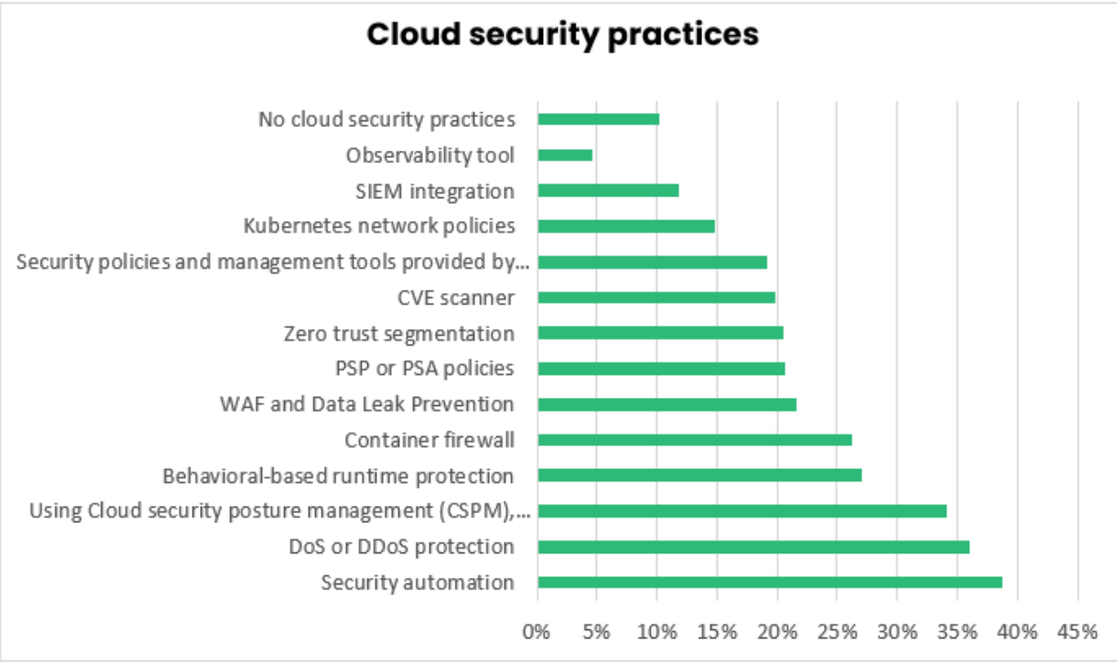
In APAC countries, the most common current security practices include automation (39%), DoS or DDoS protection (36%), or cloud (CPSM, CWPP, or CNAPP) solutions (34%). Security automation is the most consistently cited practice, with at least 25% of respondents in all APAC countries and 53% in Indonesia relying on it.

While Kubernetes network policies were a less popular solution in general (15% across the APAC region), they were more popular among China (33%) and Singapore (32%) respondents.

Cloud (CPSM, CWPP, or CNAPP) solutions were extremely popular in Indonesia (59%), China (49%), and India (45%), but were only used by 13% of both Japanese and South Korean respondents, and less than a quarter of Australians (23%).

A third of Japanese (33%) respondents and a fifth of Australian (21%) respondents reported having no current cloud security practices.

An interesting difference to IT decision makers' cloud security practices in the US / Europe is the lack of popularity of container firewalls as a security measure among APAC professionals. While Firewall has consistently been the most popular practice in the EMEA and US regions (41% in 2024 and 38% in 2023), it is significantly less popular in APAC countries (26%).



Edge Security

Across the APAC region, most respondents (62%) reported at least one Edge-related security incident in the past year, aligning with corresponding US / Europe data for 2024.

India and Indonesia were the most severely affected, with 35% and 31% of respondents reporting five or more Edge-related security incidents respectively. While 18% of respondents in Singapore reported not to have been affected, some 72% reported between 1 and 4 Edge-related security incidents.

IT security personnel reported the highest levels of vulnerability. More than a third of IT security directors (35%) had experienced between 6 and 10 Edge-related incidents. A quarter of SOC Managers (25%) had experienced 6-10 cloud-related incidents, and 26% reported 5 or more Edge-related incidents.

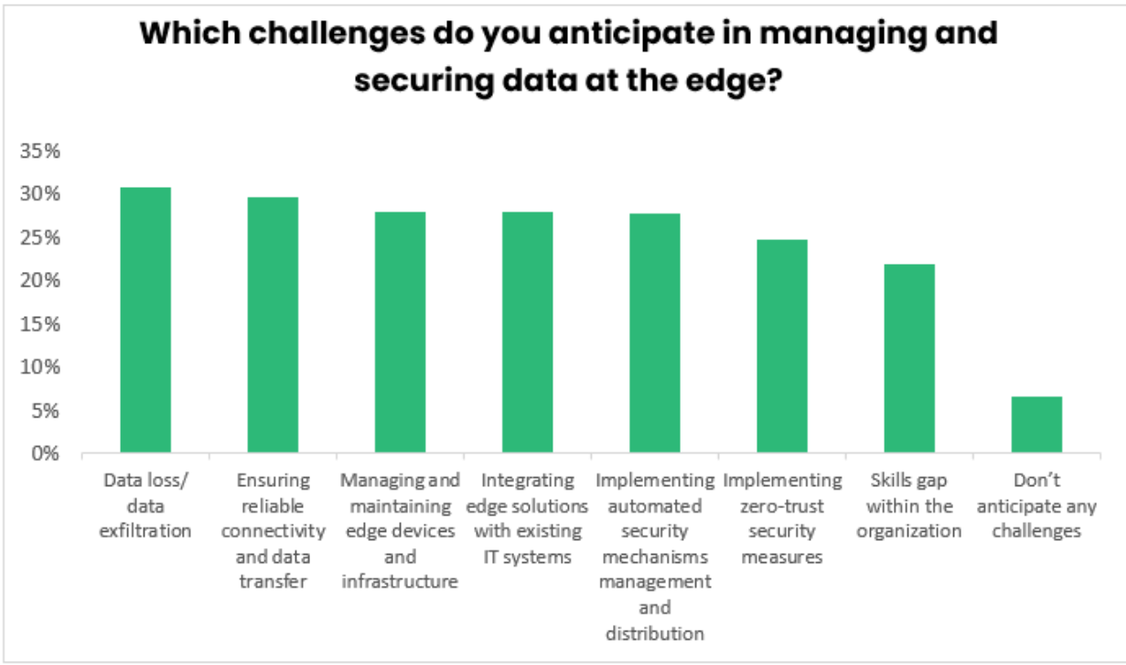
On average, IT decision makers in APAC countries spend a third (30.9%) of their overall IT budget on cloud native security, suggesting that it is considered an operational priority.

Spending was particularly high in Indonesia (42.5%), India (36.8%), and Singapore (34.2%). Chinese respondents also reported a higher-than-average spend (31.8%).

Across the region, ensuring data privacy and compliance with regulations (34%), data loss, data exfiltration (31%), and ensuring reliable connectivity and data transfer (30%) are anticipated to be the top challenges in managing and securing data at the edge.

In China, integrating edge solutions with existing IT systems (37%) and implementing automated security mechanisms management and distribution (37%) were considered the two most important challenges, versus an APAC average of 28% respectively.

In Singapore, implementing zero-trust security measures (44%) is considered a top challenge, versus an APAC average of 25%.



Supply chain security

In-house auditing of vendors' software is deemed crucial for mitigating supply chain attack risks.

Across the APAC markets, nearly one in four IT decision makers believe that Software Bill of Materials (SBOM) depth / quality / security (24%) will become more of a priority for them over the next 12 months. This is followed by increased goals on government-recognised supply chain related security certifications (21%), goals on build quality (19%), SBOM availability was voted a lesser priority (8%).

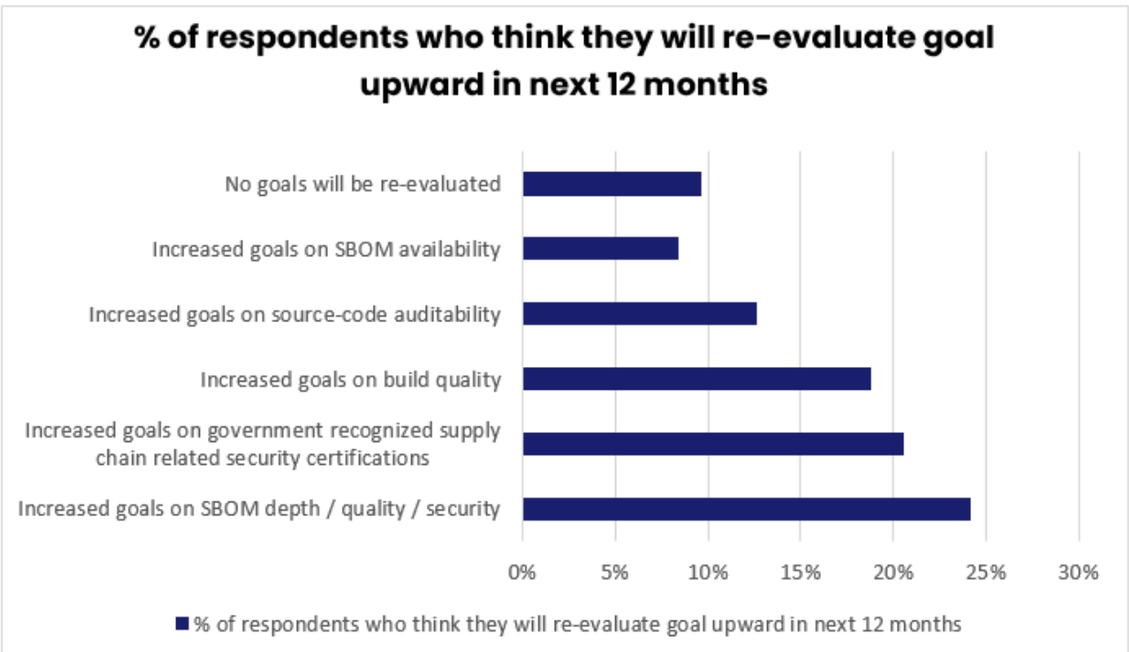
Especially IT professionals in China expected increased attention on SBOM depth / quality / security (42%), followed by decision makers from Indonesia (30%). In Singapore, IT decision makers considered goals on build quality the highest priority over the next months (28%), similarly in India (25%) and Australia (24%).

Across the different levels of seniority, priorities also varied, with those working on a board, manager, or director level focusing on SBOM depth / quality / security to increase (36%), while chairmen considered government-recognised supply chain related security certifications (37%) as a priority – suggesting that senior-level decision makers are aware of the potential impact software supply chain-related government policies might have on business operations.

To mitigate supply chain risks, IT decision makers prioritise leveraging vendor-backed software (44%) and certifying software build processes (39%).

IT professionals in Singapore rate leveraging principal vendor backed software especially high (68%).

Significantly diverging from other APAC countries, nearly a quarter of Japanese IT professionals (24%) indicate that they have not taken any measures against supply chain risks.



Methodology

The 2024 APAC edition of this trend report is based on a survey of 900 IT engineers, architects, developers, security managers, and directors. It takes a holistic perspective of the wider region by polling quantitatively and qualitatively across China, Singapore, India, Japan, South Korea, Indonesia, and Australia.

It compares how professionals in each of these markets may differ in their approach to cloud and cloud native technologies, while revealing the state of adoption. The seniority of those polled ranges from C-Suite to IT decision makers.

Like the US / Europe edition of the report, it explores the regulatory push for supply chain security, identifies potential areas that may become higher priorities in the next 12 months, and delves into organisations' intentions to review their own software supply chain for increased security. Additionally, it investigates the prevalence of cloud workloads, cloud-related security incidents, and major cloud security concerns. It also explores questions around Generative AI security.

It touches upon the importance of skills, tools, data integrity, and open source platforms in addressing security gaps and decision-making regarding cloud migration. It concludes with an inquiry into the percentage of IT spending allocated to cloud and cloud native security and current cloud security practices employed by organisations.