APAC Edition

THALES
Building a future we can all trust

2024 CLOUD SECURITY STUDY

Boom Times for the Cloud: Is Security Ready?

#2024CloudSecurityStudy

cpl.thalesgroup.com

SUPPLEMENT TO GLOBAL EDITION

This report shares findings and insights from the **2024 Thales Cloud Security Study** and focuses on results specific to the **Asia-Pacific (APAC) region.** Responses from 897 security and IT management practitioners and leaders from Australia, Hong Kong, India, Japan, New Zealand, Singapore and South Korea are compared to those of their global counterparts. While rapid cloud advances are driving opportunities for innovation, complexity-related risks and threats to data resilience are also growing. With these parallel advances in innovation and risk, opportunity and potential for harm, cloud security is cited as a top security concern in the APAC market.

This report looks at the responses from regional APAC enterprises regarding the factors driving these opportunities and concerns. While APAC respondents show similarities to the global survey population, this report notes differences where applicable.

S&P Global
Market Intelligence

Source: 2024 Data Threat Report custom survey from S&P Global Market Intelligence, commissioned by Thales.

Sponsored by

CLICO

edvance
value added distributor

EXCLUSIVE NETWORKS

Key findings

Cloud-based resources are top attack targets

Among APAC respondents,

- **30%** prioritized Cloud Storage
- **29%** prioritized SaaS applications
- **27%** prioritized cloud-hosted IaaS and PaaS apps

as most frequently chosen as the top targets for cyberattacks, in line with global responses.

Cloud data breaches remain high for APAC

15%

About one in seven APAC respondents (15%) experienced a cloud data breach in the last 12 months, similar to 14% globally. Overall, cloud breach history remains high, with 44% in APAC and 44% globally reporting at least one prior cloud data breach. Human error remains a top reason for cloud breaches.

Cloud security is a top concern, and it leads security spending plans

Cloud security is the second-most-pressing current security concern (63%) and **the top emerging security concern (73%) among APAC respondents.** It is also the top security spending category in both APAC (33%) and globally (33%).

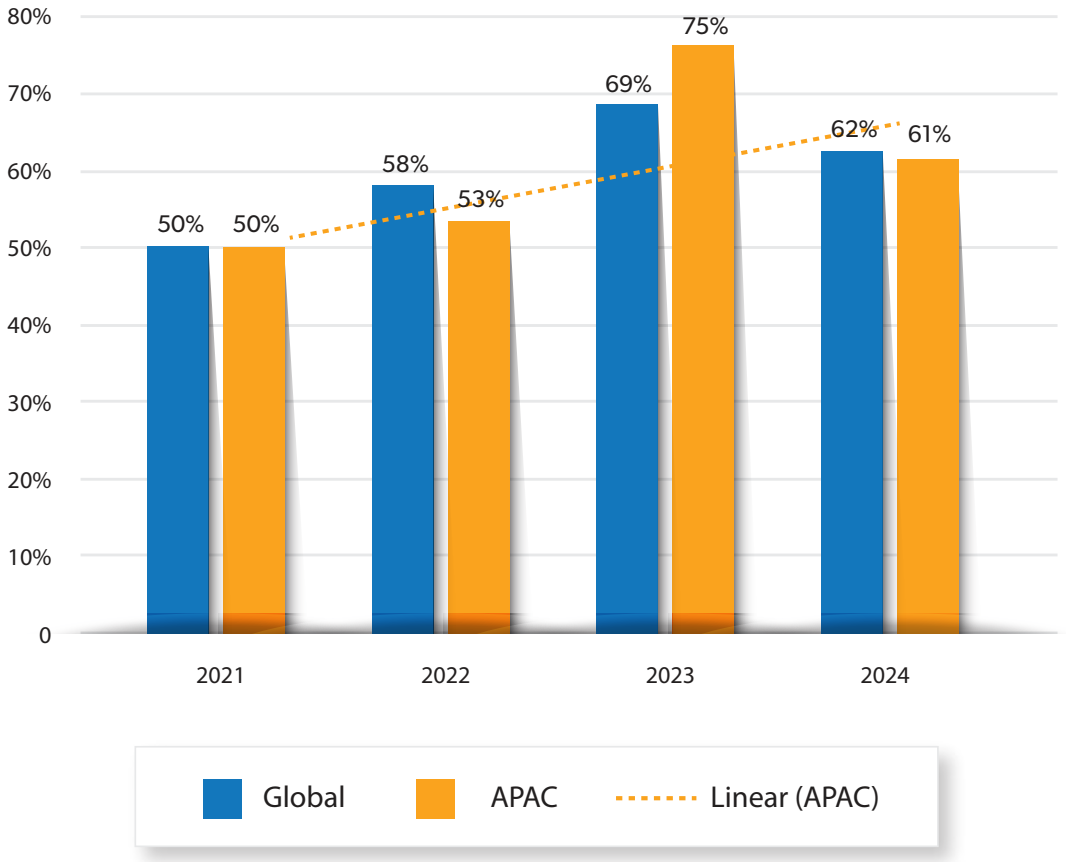
73%

Cloud complexity is a significant challenge to compliance and privacy

49%

Almost half (49%) of APAC respondents agree that securing the cloud is more complex than on-premises environments. APAC respondent organizations on average use just over two public cloud providers; over two-thirds have more than 25 SaaS apps in use.

The concentration of sensitive data in the cloud is increasing



Source: S&P Global Market Intelligence 451 Research's Cloud Security Surveys 2021-2024

Over half (61%) of APAC organizations said that at least 40% of their cloud data is sensitive, compared to 50% of respondents in 2021. This resembles global trends, where the figure rose to 62% from 50% over the same period.

Sensitive data in the cloud is increasing in volume and concentration

In 2024, 61% of APAC organisations say that at least 40% of their data in the cloud is sensitive, up from 50% of respondents in 2021, similar to worldwide numbers. Not only is the concentration of sensitive data increasing, but so is the sheer amount of data in the cloud as enterprises take advantage of the capabilities of SaaS and IaaS/PaaS environments. This growing dependence on cloud environments for critical workloads tilts the balance of sensitive data further toward the cloud, resulting in ever-greater concentrations and volumes of sensitive data in the cloud.

Further, given cloud capabilities, enterprise applications effectively operate in multinational contexts. The distribution of data across a single logical application may present multiple mandates from different jurisdictions. Multinational organisations may be subject to multiple jurisdictions and mandates, tightening the definition of sensitive data and how it is handled.

The occurrence of cloud data breaches in APAC remains high, similar to global figures: 15% of APAC respondents reported a cloud data breach in the last 12 months (versus 14% globally), while 44% have a history of at least one cloud data breach, in line with the global figure.

KEY STATISTIC

The occurrence of cloud data breaches in APAC remains high, similar to global figures: 15% of APAC respondents reported a cloud data breach in the last 12 months (versus 14% globally).

15%

In 2024, among APAC respondents whose organizations failed a compliance audit, 87% reported some breach history, slightly higher than the global result. In contrast, for APAC organizations that passed all compliance audits, only 18% reported any breach history (lower than the global figure), and only 2% experienced a breach in the past 12 months (slightly lower than the global result).

Data breach severity, as measured by the proportional amount of sensitive data lost, is trending upward. Data breaches are increasingly multifaceted: unauthorised exposure to data may enable adversaries to exfiltrate or tamper with data, and to extort the targeted organization or hold data for ransom, attacking confidentiality, integrity and availability.

Human error is a top reason for cloud breaches, cited by nearly one-third of respondents in APAC (29%) and globally (31%). APAC respondents report that, on average, 50% of employees use strong authentication to access cloud applications. Yet the failure to use MFA can be costly. In APAC, 14% of cloud data breaches are attributed to a lack of MFA and strong authentication for privileged accounts, compared to 17% globally.

Cloud assets a top security concern – and attack target

Cloud development, scale and complexity have made cloud assets top targets for attack. The largest proportion of APAC enterprises cite cloud storage (30%) and cloud-delivered SaaS applications (29%) as top targets for cyberattack. The urgency and scale of cloud security is further driven by complexities related to new functions and exposed services available.

Approximately two-thirds of APAC enterprises say cloud security is both a pressing current security discipline for their organization (63%) and a top emerging security concern (73%), similar to global respondents. While cloud and SaaS environments offer security advantages such as automation and immutability, the complexities of deploying across multiple toolsets with increasing quantities and concentrations of sensitive data have added to both APAC and global enterprise urgency. The changing nature of cloud workloads for generative AI and initiatives such as digital sovereignty are driving enterprise concerns. For these reasons, APAC respondents prioritize cloud security ahead of other issues such as regulation, identity and access management (IAM), security operations and on-premises infrastructure security.

Cloud Complexity is Increasing

The same features and benefits that make cloud so popular also cause much of the underlying complexity for security. Part of the reason for that complexity is the sheer number of cloud resources that organizations must manage. The average reported number of IaaS/PaaS providers has dipped a little in the most recent survey, but on average, APAC enterprises still use 2.1 production cloud providers for their IaaS/PaaS-based applications. Each cloud provider offers many products, adding to the complexity. In addition, the number of SaaS vendors shows no sign of slowing or consolidation. More than two-thirds (68%) of APAC enterprises have more than 25 SaaS applications in use, compared to 66% globally; over one-third (34%) have more than 50 SaaS applications, versus 31% globally. Among APAC respondents, 62% use AWS (versus 61% globally), 49% use Microsoft Azure (versus 49% globally) and 30% use Google Cloud Platform (versus 35% globally). Notably, one-fourth of APAC respondents use Alibaba, compared to just 13% globally.

Nearly half (49%) of APAC respondents agree that securing the cloud is more complex than on-premises environments, versus 51% of global respondents. Both in APAC and globally, one-third (33%) of respondents say cloud security is their top spending priority. Workforce IAM is the No. 2 spending priority for both APAC (32%) and globally (29%). However, SaaS security is less of a spending priority for APAC, coming in sixth overall (19%), presenting a bit of a disconnect and a potential opportunity to revisit overall security priorities.

KEY STATISTIC

Nearly half (49%) of APAC respondents agree that securing the cloud is more complex than on-premises environments, versus 51% of global respondents.

49%

DevOps and cloud security: Secrets management and cooperation are key

While cloud services may be a permanent fixture, the workloads operating within them are increasingly short-lived. For enterprises following DevSecOps approaches, security and risk management practices must consider the dynamic nature of development in which previously secured workloads may be quickly replaced or renewed, driven by different requirements. Security architectures must also be flexible and loosely coupled to the underlying cloud workloads they secure as these environments change. APAC respondents attribute just over half (56%) of cloud data breaches to known and unknown vulnerabilities, and 43% of APAC respondents report that secrets management is one of their greatest DevOps challenges. One encouraging sign is that (55%) of APAC respondents have a formal security champions program; establishing security champions might be considered an initial step toward integrating security, developer and operator teams.

KEY STATISTIC

APAC respondents attribute 56% of cloud data breaches to known and unknown vulnerabilities, and 43% report that secrets management is one of their greatest DevOps challenges.

56%

Sovereignty and Cloud Migration – full digital sovereignty and repurchasing are top choices

Future-proofing portability via full data and software sovereignty (33%) is the top driver for digital sovereignty initiatives among APAC respondents, above the need to satisfy privacy frameworks (20%) or local market conditions (17%). Whereas data sovereignty enables enterprises to choose where sensitive data is processed and stored and what independent encryption schemes are used, full digital sovereignty enables enterprises to switch cloud providers or repatriate workloads with data still accessible in an open format usable by equivalent open-source programs.

Like their global counterparts, APAC respondents report contrasting priorities between their current approach to cloud migration and their preferred methods to achieve cloud sovereignty. When asked about their current migration strategy for IaaS or PaaS cloud applications, APAC respondents' top response is to "repurchase and shift" (31%), replacing on-premises applications with SaaS or off-premises hosted versions. This is followed by "lift and shift" (26%), migrating on-premises applications to off-premises/cloud environments with minimal changes to the code, and only 22% saying they primarily rearchitect or refactor their applications. Yet, when asked about their desired path to achieve sovereignty, the largest proportion (27%) say they would refactor or rearchitect their applications, ahead of leveraging SaaS (21%) or workload repatriation or migration (14%). In their efforts to achieve digital sovereignty, enterprises must strike a balance between maintaining independence from any given provider and meeting their overall business objectives.

Pathways to better cloud security

The growth of cloud workloads, especially given newer initiatives in generative AI, presents new challenges, and organizations need to proactively address both the potential benefits and security challenges of cloud technologies. APAC respondents, like their global counterparts, suggest some pathways toward better cloud security.

Compliance matters. In this year's studies, the factor most strongly correlated to lower breach occurrence is success in compliance audits. Enterprises that passed all security audits had significantly lower incidence of cloud data breaches in the last 12 months. Overall, 15% of APAC respondents reported a cloud data breach in the last 12 months, compared to only 2% of those that passed all audits.

Prioritize investment in cloud security tooling. Like their global counterparts, 33% of APAC respondents say they are spending on cloud security for IaaS/PaaS, and 59% say they use cloud security solutions such as cloud-native application platform protection (CNAPP). Multicloud organizations using multiple IaaS and SaaS providers could also benefit from deploying key management as a service. However, APAC respondents identify workforce IAM (31%), endpoint security (31%) and network security (30%) as most effective at protecting sensitive data from cyberattacks, with cloud security ranking fourth (27%).

KEY STATISTIC

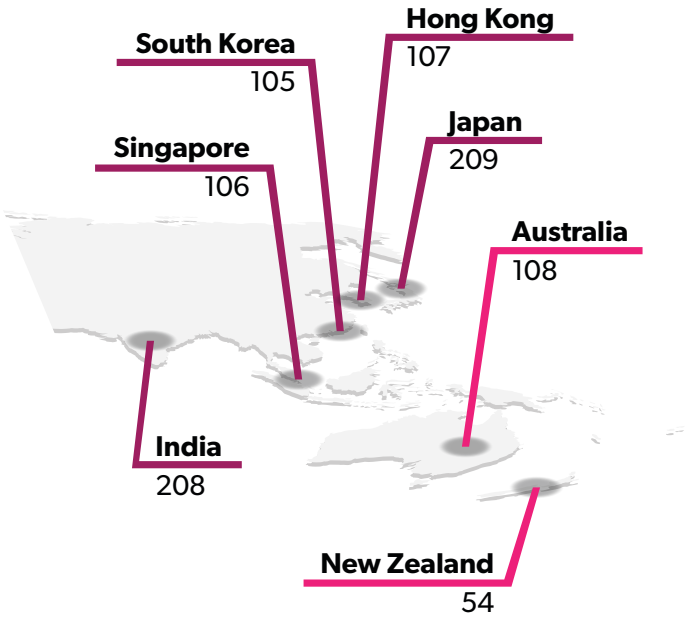
Like their global counterparts, 33% of APAC respondents are spending on cloud security for IaaS/PaaS, and 59% say they use cloud security solutions such as cloud-native application platform protection (CNAPP).

33%

Strengthen developer and security partnerships. New threats and vulnerabilities from cloud operations will require stronger developer, operator and security practitioner partnerships. Establishing security champions might be considered a first step toward integrating security, developer and operator teams; encouragingly, 55% of APAC respondents report having a formal security champions program, similar to the global figure. Another positive sign is that nearly half (52%) of APAC respondents report aligning their product and security roadmaps, compared to 49% globally. Complex environments are best secured at early design phases, where preventative controls and guardrails can limit the likelihood and scope of any single incident.

About this study

This research is based on a subset of the global survey of 2,961 respondents that was fielded in November and December 2023 via a web survey aimed at professionals in security and IT management. This subset comprises targeted populations in Asia-Pacific markets — Australia, Hong Kong, India, Japan, New Zealand, Singapore and South Korea — for a total of 897 respondents across 36 industries. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100 million. The majority of respondents (80%) were affiliated with organizations reporting annual revenue between US$100 million and US$999.9 million. This research was conducted as an observational study and makes no causal claims.



Revenue	Number of Respondents
$100m to $249.9m	89
$250m to $499.9m	257
$500m to $749.9m	197
$750m to $999.9m	178
$1 Bn to $1.49 Bn	81
$1.5 Bn to $1.99 Bn	34
$2 Bn or more	61

Industry Sector	Number of Respondents	Industry Sector	Number of Respondents
Manufacturing	140	Media/Marketing	76
Financial Services	126	Government	69
Retail/Hospitality	120	Transportation	50
Healthcare	95	Telecommunications	36
Services	88	Energy & Utilities	31
Technology	66		

THALES

Building a future we can all trust

For contact information, please visit
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/apac-cloud-security-research