APAC Edition

THALES
Building a future we can all trust

2024 DATA THREAT REPORT

Navigating New Threats and Overcoming Old Challenges

#2024DataThreatReport
cpl.thalesgroup.com

SUPPLEMENT TO GLOBAL EDITION

In this report, we share key findings from the **2024 Thales Data Threat Report (DTR)**, focused on the **Asia-Pacific (APAC) region,** and briefly discuss differences between APAC and global responses, along with enterprise observations and a summary of the threat landscape.

S&P Global
Market Intelligence

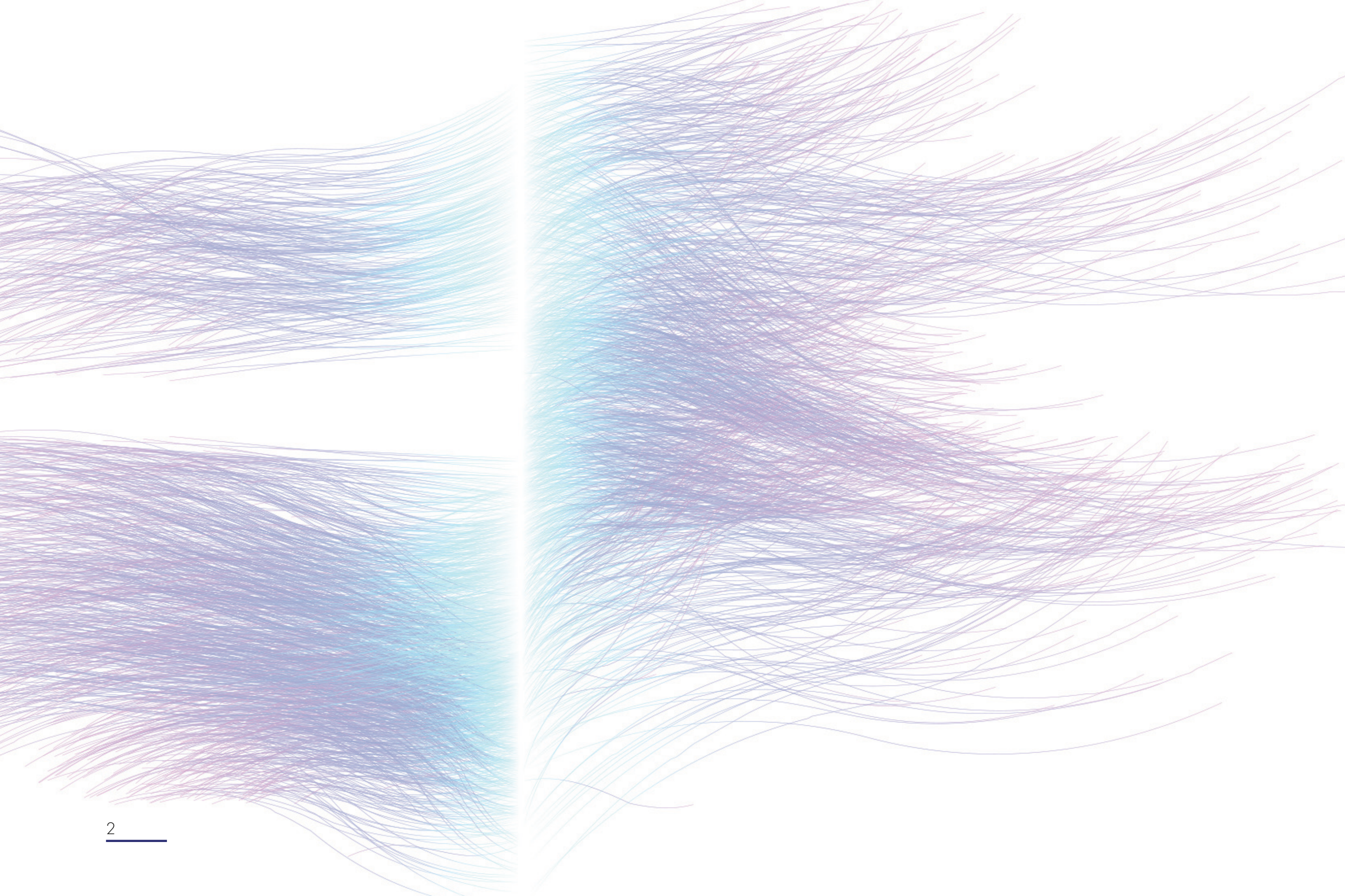
Source: 2024 Data Threat Report custom survey from S&P Global Market Intelligence, commissioned by Thales.

Sponsored by

edvance
value added distributor

EXCLUSIVE
NETWORKS

netpoleon
Network • Security



Key Findings

Data Breach Trends and Threats

Nearly half (48%) of APAC respondent enterprises have had at least one cloud data breach in their history, compared to 49% of global respondents. Globally, the proportion of respondents reporting a recent breach decreased from 24% in 2021 to 15% in 2024. **APAC respondents reflect a slightly smaller decrease, from 22% reporting a recent breach in 2021 to 16% in 2024.**

48%

More than a quarter (28%) of APAC respondent enterprises have experienced a ransomware attack. Half of that group (14%) have been attacked in the last 12 months. Global percentages are similar: 28% have had a ransomware attack at some point, and 12% have been attacked in the last 12 months. **Despite high ransomware attack rates, planning remains poor, both in theory and in practice, in APAC and globally.** Among APAC respondents who did not experience a ransomware attack, only 20% said they would follow a formal ransomware plan. In practice, for APAC respondents who did experience an attack, only 18% followed a formal plan. Global figures are similar here, too.

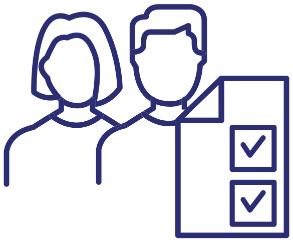
28%

Both APAC and global respondents reported vulnerability exploitation as the leading cause of cloud data breaches. Known and unknown vulnerabilities caused 30% and 27% of these breaches, respectively, among APAC enterprises, in line with global responses at 28% and 24%, respectively.

Human factors still have significant bearing on cloud data breaches: APAC enterprises reported that 29% were caused by user and operator errors. A further 14% reported that the lack of strong MFA caused their cloud data breaches.

29%

Identity Complexities and Compromise



Customers make up about one-sixth (16%) of all users accessing corporate cloud, network and device resources among both APAC and global respondents. Vendors and suppliers account for a similar proportion, at just over 15%.

16%

Among APAC respondents who identified external identity as a top source of emerging security concern, two-thirds (66%) reported that security consistency between workforce and non-workforce identities is their top challenge to enabling external users.

66%

Increasing DevOps Challenges

58%

Among APAC respondents who identified cloud/DevSecOps as a top area of emerging security concern, **secrets management is the number one DevOps challenge, cited by 58%** — similar to the global figure of 55%.

Operational complexity remains a security concern. Both in APAC and globally, 53% of respondents reported that their organization uses five or more key management systems. This has slowly progressed downward since 2021, when 58% of APAC respondents reported using more than five key management solutions. **This suggests that APAC organizations and their global counterparts need to further simplify operations.**

5+

APAC respondents reported similar levels of DevSecOps organizational maturity as their global peers. Just over half (55%) of APAC respondents reported having a formal security champions program, and 52% reported having alignment between security and product roadmaps. Global figures were 53% and 49%, respectively.

Risks to Emerging Technologies

57%

More than half (57%) of APAC respondents cited IoT as one of their top emerging security concerns, in line with 53% of respondents in North America. Among APAC respondents who identified IoT as an area of emerging security concern, nearly three-fourths (72%) said patching and updating their IoT environments is the greatest IoT/OT security challenge. A nearly identical proportion (73%) said they would protect IoT and OT environments by using existing IT security practices.

47%

The generative AI boom is underway: 49% of global respondents and 47% in APAC said they are in either the integration or enablement phases of adopting AI. When it comes to AI, the fast-changing ecosystem is the greatest source of concern, cited by 68% of APAC respondents.

Enterprise Observations

This year's DTR provides additional insights into IT organizations and enterprise security in the APAC region. The need for data security as a discipline remains diffused throughout the enterprise. Functions such as compliance, go-to-market, supply chain and design all incorporate data security across multiple technologies in cloud, IoT and GenAI applications, for both internal and external collaborators.

Security and compliance initiatives are converging on common inputs, processes and outcomes. Through the years, DTR findings have shown a stronger correlation between compliance achievement and reduced breaches. In 2024, of the APAC respondents whose organizations failed a compliance audit, 86% reported at least one prior breach in their history, and 34% had a breach in the last 12 months. Conversely, among APAC respondents whose organizations passed all compliance audits, 15% reported a breach history and just 2% reported a data breach in the last 12 months. Global results also favored security-compliant respondents: Just 21% of global respondents whose organizations passed all compliance audits reported a data breach history, and just 3% had a breach in the last 12 months.

KEY STATISTIC

In 2024, of the APAC respondents whose organizations failed a compliance audit, 86% reported at least one prior breach, and 34% had a breach in the last 12 months.

86%

KEY STATISTIC

Conversely, among APAC respondents whose organizations passed all compliance audits, 15% reported a breach history and just 2% reported a data breach in the last 12 months.

15%

Compliance is arguably different from security, but both disciplines use many of the same techniques. Increasingly, regulatory oversight blurs distinctions between compliance and security diligence. For example, compliance standards such as AICPA SOC2 Type 2 and ISO27K require organizations to demonstrate controls over time (a characteristic typically associated with security) rather than at a single point in time. Automation will continue to drive improvement in this area, such as through the application of security as code. Among APAC respondents prioritizing DevSecOps, 34% said that their configuration, compliance and security controls were defined as code, similar to 38% global. This report shares further insights on enabling developers and operators to achieve better security and service outcomes.

The Threat Landscape

In APAC, as in the rest of the world, the attack landscape remains vast and growing. **Globally, 93% of respondents said they were experiencing an increase in attacks, similar to 95% of APAC respondents.** Also similar to global results, APAC respondents identified malware (44%), phishing (36%) and ransomware (35%) as the top three fast-growing attack types. Globally, malware, phishing and ransomware were cited by 41%, 36% and 32%, respectively.

For APAC enterprises, external threat actors present the greatest concern — external ideological attackers at 77% and external geopolitical attackers at 75%. These figures are similar to global trends, and they also reflect longer-term changes in focus from internal to external threat actors. In 2021, 65% of APAC respondents cited insider threats, such as human error and malicious insiders, as the greatest type of threat actor. When considering cloud data dangers, 24% identified cloud management infrastructure as a top target of attack. Two-fifths (41%) of APAC respondents cited attacks against identities in workforce identity access management or underlying identity infrastructure such as identity providers, similar to 40% of global respondents.

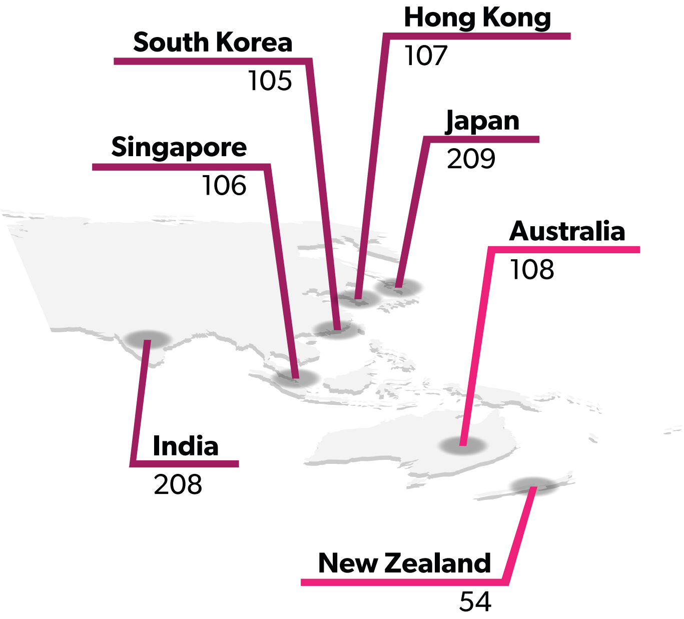
Ransomware response remains a challenge. 28% of APAC respondents have experienced a ransomware attack, and 14% had been attacked in the last 12 months. Among those who were attacked, 24% of attacks had some impact on external operations. The response to ransomware attacks continues to show need for improvement, with just 18% saying they executed a formal ransomware response plan. Of those who were not attacked with ransomware, just 20% said they would execute a formal ransomware response plan. Ransomware payment lingers as a response, with 8% of APAC respondents saying they have paid or would pay a ransom.

The complexity of cloud resources present among users, operators and developers continues to grow. Four in five APAC respondents (80%) reported that their organization uses two or more public cloud providers for production workloads, with 30% of APAC enterprises using three or more cloud providers. In addition, 34% of APAC respondents reported that their enterprise uses 50 or more SaaS apps, above the global figure of 31%. This comparison is roughly reversed from 2021, when 24% of APAC enterprises were using 50+ SaaS apps, versus 27% of global enterprises. The inherent complexity of cloud technologies, as well as the growing use of multiple cloud environments, may indicate why 49% of APAC enterprises said it is more complex to manage privacy and data protection regulations in cloud environments versus on-premises.

Yet this comparison is certainly not static. Technologies are emerging that blend or abstract differences between cloud and on-premises environments and operations. This year's study asked respondents to prioritize their emerging areas of security concern. **While 73% of APAC respondents ranked cloud and DevSecOps among their top emerging concerns, external identity/access management and digital sovereignty took second and third places, respectively, in line with global responses.**

About This Study

This research was based on a subset of the global DTR survey of 2,961 respondents that was fielded in November and December 2023 via web survey. This subset was composed of targeted populations in seven APAC markets (Australia, Hong Kong, India, Japan, South Korea, New Zealand and Singapore for a total of 897 respondents across 36 industries) aimed at professionals in security and IT management. 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, with the majority of respondents (80%) 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-data-threat-report