APAC Edition

THALES
Building a future we can all trust

2022 Thales Cloud Security Study

The Challenges of Data Protection in a Multicloud World

#2022CloudSecurityStudy

cpl.thalesgroup.com

Introduction

The 2022 Thales Cloud Security Study polled nearly 2,800 IT professionals in 17 countries in five regions (USA, Canada, Europe, Asia Pacific, and Latin America). The Asia Pacific (APAC) section of the report focuses on data from respondents in seven key markets in the APAC region—Australia, Hong Kong, India, Japan, New Zealand, Singapore, and South Korea— constituting 876 respondents from midsize to large enterprises. The study examines major cloud and cloud security trends that are reflected in the survey data across the region.

In this report, we consider trends seen in APAC, how they compare globally and with other regions – as well as with prior research – and how all these factors are manifested in APAC. Unless noted otherwise, 'respondents' in this report refers to APAC-based respondents.

Contents

Key Findings 04

APAC Shifts Into Multicloud Gear 07

Cloud Complexity is a Major Concern 08

Cloud Security Policies and Standards 09

Failed Audits, Data Breaches, and Cloud Data Breaches 10

Encryption in the Cloud 11

Encryption Key Management 12

Zero Trust 13

Conclusion 14

About This Study 15

Key Findings

- Most APAC organisations have now adopted a multicloud approach, with 60% of respondents indicating more than one cloud provider. Customers are using a wide range and variety of SaaS, IaaS, and PaaS cloud solutions in their environments.
- Increasing cloud complexity is a major concern, echoed globally by virtually all respondents.
  - o Significant workloads and data remain outside of cloud environments in APAC, four percentage points lower than the global number.
- Cloud security policies and standards are key concerns, with strong trends toward centralised cloud policy control and enforcement evident.
- Failed compliance audits are on an upward trajectory, with a growing number of audit failures over 2021.
- Data breach rates were significantly lower than global averages, although improvements in cloud data breaches and failed audits were also lower.
- Encryption technologies are important, particularly so from a regulatory perspective, although adoption of these technologies remains relatively low, both regionally and globally.
  - o Key management solution sprawl is a key issue for organisations worldwide, creating additional complexity and increasing risk.
- APAC organisations are embracing zero trust, particularly in cloud environments, although increases in adoption are modest.

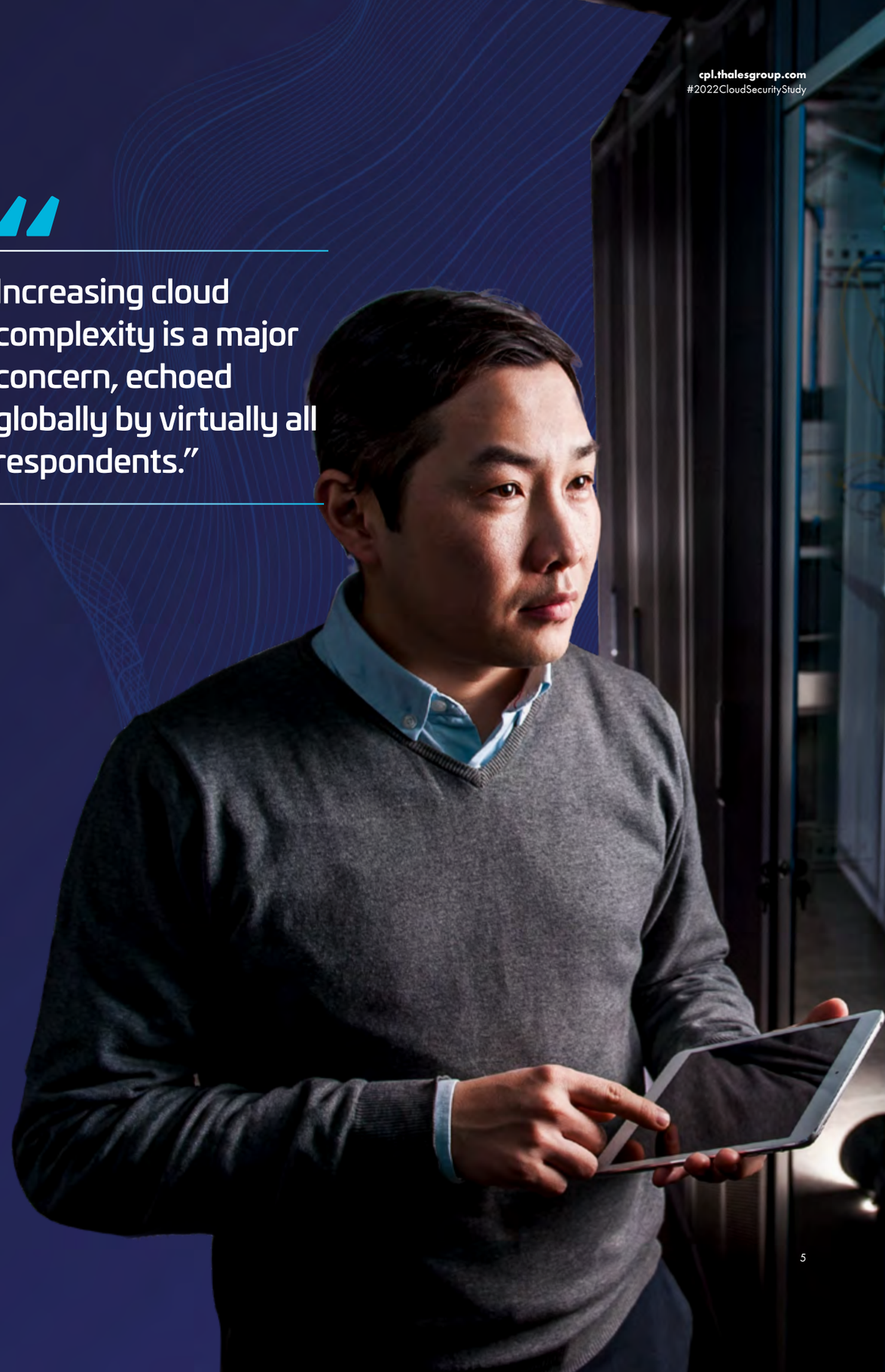
43%

of respondents reported failing an audit within the past 12 months, identical to the global percentage.

55%

of respondents reported using 5 or more key management solutions.

“Increasing cloud complexity is a major concern, echoed globally by virtually all respondents.”



> **Like much of the world, enterprises reported a variety of approaches to cloud adoption."**

APAC Shifts Into Multicloud Gear

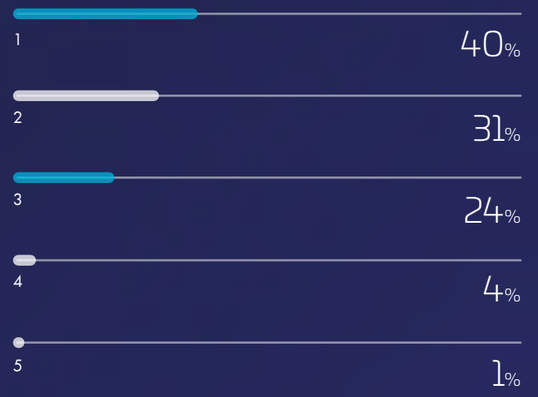
Multicloud use is gaining, with 60% of respondents reporting more than one cloud (SaaS/IaaS/PaaS) provider, 8% lower than the worldwide number. Survey respondents reported using a mix of SaaS, IaaS, and PaaS cloud platforms.

Like much of the world, enterprises in APAC reported a variety of approaches to cloud adoption. Migrations from existing applications to IaaS/PaaS show repurchase and shift is the most popular option (33%), followed by lift and shift/migrate existing apps (22%) and re-architect/refactor apps (16%), similar to 2021 findings and consistent with other regions.

FIGURE 1

Multicloud Growth

NUMBER OF CLOUD IAAS PROVIDERS USED IN A PRODUCTION CAPACITY



Source: 451 Research's 2022 Cloud Security custom survey.

> **Survey respondents reported using a mix of SaaS, IaaS, and PaaS cloud platforms."**

Cloud Complexity is a Major Concern

While substantial workloads and data are distributed among multiple cloud providers, significant data remains outside of cloud environments."

The diversity of multicloud environments contributes to operational and security complexity. Nearly half of respondents believe that managing privacy and data protection regulations in a cloud (multicloud/hybrid) environment is more complex than on-premises networks, and while substantial workloads and data are distributed among multiple cloud providers, significant data remains outside of cloud environments. Only 19% of respondents have more than 60% of their data stored with external cloud providers, four percentage points lower than global results. This likely indicates a hesitancy to move to cloud in the region. The high number of SaaS applications also contributes to cloud complexity, with 16% of respondents reporting over 100 and 31% reporting over 50.

Only

19%

of respondents have more than 60% of their sensitive data stored with external cloud providers.

A high number of SaaS applications also contributes to cloud complexity."

Cloud Security Policies and Standards

This year's survey indicated a shift in how cloud security policies and technical standards are determined and enforced. Nearly half (47%) of respondents reported that cloud security policies are centrally defined by the security team, but definition of technical standards and policy enforcement are left to individual cloud delivery teams, a 5% increase over 2021. More than one-third (38%) reported that cloud security policies, standards and enforcement are all centrally controlled by the security team, and 15% reported that all three are left to individual cloud delivery teams, a 7% decrease over 2021. Japan showed the highest increases in centralisation (14%), compared with the APAC average of 7% and 2% globally; we saw similar shifts in other APAC countries. Survey results clearly indicate a shift toward centralised definition, control and enforcement of cloud policies, which is likely a sign of increasing requirements for managing complex multicloud deployments and consistent with global findings.

Failed Audits, Data Breaches, and Cloud Data Breaches

Failed compliance audits were on the increase, with 43% of respondents reporting a failed audit within the past 12 months, identical to the global average. Hong Kong and India reported the highest audit failure rates (50% and 49%), and South Korea reported the lowest failure rate (39%). Data breaches were lower, with 32% of organisations reporting a breach in the past year, down 7% from 2021 and 11% lower than the global average, placing enterprises in this region among the lowest rates in the world. APAC cloud data breaches and failed audits showed some improvement, 33% of APAC respondents have experienced a data breach or failed an audit involving data and applications stored in the cloud this past year, down 4% from 2021 and 2% lower than the rest of the world. It should be noted that low failed audit rates may be the result of less mature compliance regimes and lower enforcement requirements in the region.

43% of respondents reported a failed audit within the past 12 months."

Encryption in the Cloud

Encryption technologies are critical security controls needed to protect sensitive data from cyberattacks. Respondents cited data-at-rest encryption, tokenization and data masking, data-in-transit encryption, and key management/hardware security modules as top-ranked techniques. Importantly, 38% of APAC enterprises surveyed indicated they avoided required breach notifications thanks to "safe harbour" regulatory provisions that allow exceptions for stolen or leaked data that is encrypted or tokenized. APAC results were like other regions, with data clearly demonstrating the security and business value received from these technologies. When asked about drivers for where and how encryption is used in the cloud, 46% of respondents chose internal security architecture decisions as their primary driver, followed by regulatory compliance at 38%, comparable with global averages.

Respondents in countries subject to significant privacy regulations typically rank compliance as their most significant driver. Encryption is critical in protecting cloud environments, yet encryption of sensitive cloud data remains elusive, with only 21% of respondents indicating more than 60% of sensitive data in the cloud is encrypted, close to global averages. These findings highlight the need for enterprises to improve the adoption and maturity of this critical protection against breaches and compliance audit failures.

Only

21%

of respondents are indicating over 60% of sensitive data in the cloud was encrypted, close to global averages.

38%

of APAC enterprises surveyed indicated they avoided required breach notifications thanks to "safe harbour" regulatory provisions that allow exceptions for stolen or leaked data that is encrypted or tokenized.

Encryption Key Management

Key management is a common challenge for organisations worldwide, and key management sprawl is particularly worrisome. Only 12% of respondents reported 1-2 key management solutions, while 55% reported five or more, similar to global results. This speaks to the persistence of a problem despite the availability of solutions that can reduce complexity, lower risks, increase security efficiency and reliability, and lower costs. Organisations reported a mix of encryption key management strategies, with a 7% increase in managing keys in cloud consoles, indicating that consolidation of key management solutions to centralized platforms has begun. This reduces overall complexity and the complexity of securing cloud environments, especially for multicloud organisations that need help standardizing tools across environments.

Zero Trust

APAC organisations are embracing zero trust strategies, starting zero trust journeys that focus on access to sensitive information and functionality where controls have the greatest effect. More than three-quarters (80%) of enterprises said they are considering, evaluating, or deploying zero trust plans, and while 2022 increases were modest, this shows a continuation of the trend toward zero trust, a positive sign. Greater adoption of zero trust for cloud access was another key trend. Respondents were asked where they expect to leverage zero trust principles and techniques, and 62% cited cloud access, identical to global results.

When asked to what extent zero trust is shaping their cloud security strategy, 30% indicated a great extent, 48% reported using some zero trust concepts, and 22% indicated that zero trust did not affect cloud security strategy, in line with global percentages. Overall, survey numbers indicate slight increases in the importance of zero trust in APAC respondents year over year.

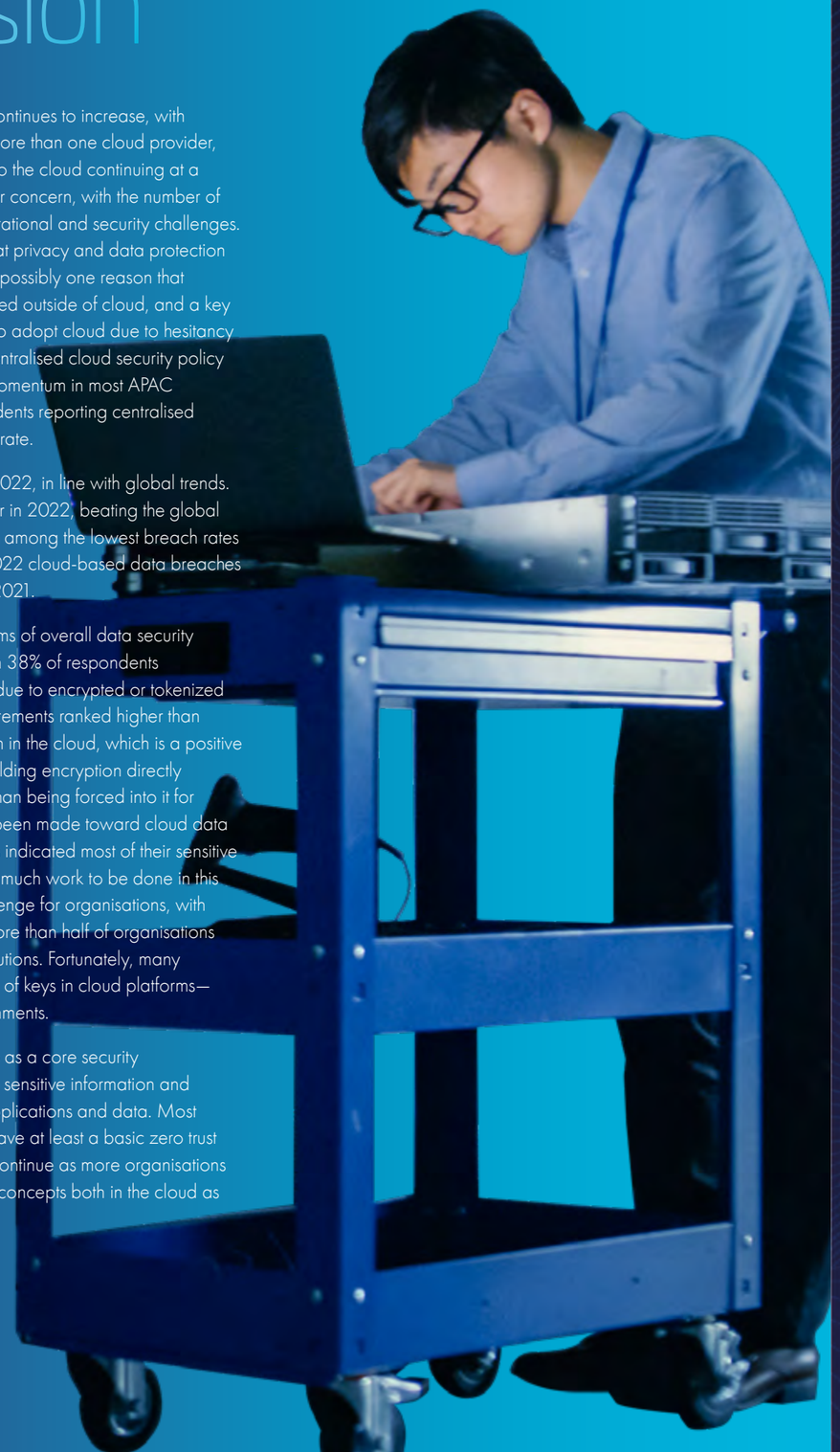
80%

of enterprises said they are considering, evaluating, or deploying zero trust plans.

22%

indicated that zero trust did not affect cloud security strategy, in line with global averages.

Conclusion



The data shows that cloud complexity continues to increase, with over 60% of APAC respondents using more than one cloud provider, and migration of business applications to the cloud continuing at a rapid pace. Cloud complexity is a major concern, with the number of multicloud environments increasing operational and security challenges. Nearly half of respondents indicated that privacy and data protection is more complex in cloud environments, possibly one reason that significant quantities of data are still stored outside of cloud, and a key indicator that organisations are slower to adopt cloud due to hesitancy in moving sensitive data. Adoption of centralised cloud security policy definition and enforcement is gaining momentum in most APAC countries surveyed, with 85% of respondents reporting centralised policy definition, well above the global rate.

Failed compliance audits increased in 2022, in line with global trends. The number of data breaches was lower in 2022, beating the global average by 11% and placing the region among the lowest breach rates in the world. APAC also fared well in 2022 cloud-based data breaches and failed audits, decreasing 4% from 2021.

Encryption of cloud data is critical in terms of overall data security and breach notification avoidance, with 38% of respondents reporting avoided breach notifications due to encrypted or tokenized data. Internal security architecture requirements ranked higher than compliance as key drivers for encryption in the cloud, which is a positive indicator that suggests organisations building encryption directly into cloud projects from the start rather than being forced into it for regulatory reasons. While strides have been made toward cloud data encryption, only one in five respondents indicated most of their sensitive cloud data is encrypted; there is clearly much work to be done in this area. Key management remains a challenge for organisations, with management "sprawl" a major issue: more than half of organisations reported over five key management solutions. Fortunately, many organisations have begun centralisation of keys in cloud platforms—particularly critical for multicloud environments.

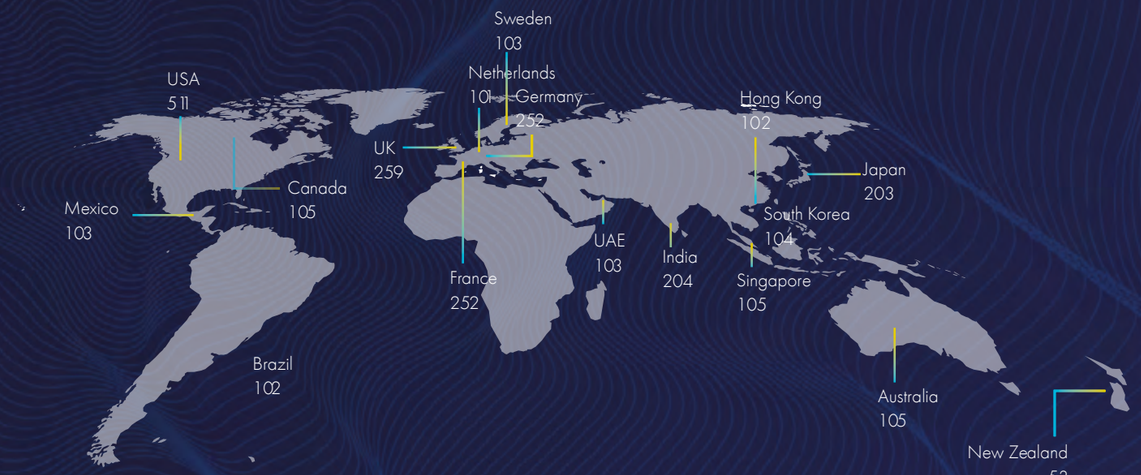
Zero Trust continues to gain acceptance as a core security methodology, with a focus on access to sensitive information and functionality—particularly so in cloud applications and data. Most APAC respondents indicated that they have at least a basic zero trust strategy in plan, a trend that is likely to continue as more organisations realise the value in deploying zero trust concepts both in the cloud as well as on premise.

About This Study

As organisations step beyond the urgent actions of the last two years, they are grappling with securing the more complex environments in which they now operate.

The global edition of the 2022 Thales Cloud Security Study looked at various aspects of these current environments in a wide-ranging survey of security professionals and executive leadership that touched on issues including accelerated digital transformation, cloud migration and the complexities of managing security in a multicloud world. The 2022 Thales Cloud Security Study is based on data from a survey of nearly 2,800 security professionals and executive leaders, including 876 respondents from the APAC region.

This research was conducted as an observational study and makes no causal claims.



Industry Sector

Manufacturing	157
Retail	154
Technology	127
Financial Services	120
Healthcare	115
Public Sector	109
Consumer Products	107
Computers/ Electronics/Software	106
Engineering	104
Federal Government	103

Revenue

$100 million to $249.9 million	162
$250 million to $499.9 million	802
$500 million to $749.9 million	865
$750 million to $999.9 million	458
$1 billion to $1.49 billion	254
$1.5 billion to $1.99 billion	58
$2 billion or more	168

Source: 451 Research's 2022 Cloud Security custom survey

THALES
Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

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