



APAC Edition

**THALES**  
Building a future we can all trust

# 2022 Thales Data Threat Report

Navigating Data Security in an Era  
of Hybrid Work, Ransomware and  
Accelerated Cloud Transformation

**#2022DataThreatReport**

---

[cpl.thalesgroup.com](https://cpl.thalesgroup.com)

---





# Introduction

Two years on, the COVID-19 pandemic continues to dramatically impact IT teams worldwide. The 2022 Thales Global Data Threat Report looked at many aspects of those impacts, with insights found from topics such as ransomware, zero-trust security strategies and cloud data security trends. This report covers respondents based in the APAC region, which we define as the nations of Australia, Hong Kong, India, Japan, New Zealand, Singapore and South Korea. This report analyzes 876 respondents from midsize to large enterprises within many diverse verticals in the public and private sectors. Unless noted otherwise, 'respondents' in this report refers to APAC-based respondents.

451 Research

**S&P Global**

Market Intelligence

Source: 2022 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

# 45%

of APAC respondents reported an increase in the number of attacks.

# 77%

of APAC respondents said they would trust their organization with their own personal data.

# Contents

---

Breaches Still Disturbingly High	4
Security Threats	6
Ransomware Planning and Response	6
Continued Era of Remote Working	7
Zero Trust Strategies Gaining Momentum	8
Cloud Momentum, Cloud Coverage Gaps	9
Most Firms Are Using a Multicloud Strategy	10
Multiple Clouds and Key Management Options Driving Complexity	11
Moving Ahead	12
About This Study	13

---



# Breaches Still Disturbingly High

Despite substantial annual spending on cybersecurity, breaches are still being reported at a disturbingly high rate: In 2022, half (50%) of respondents reported that they have experienced a security breach at some point, and of these, 32% said they had experienced a breach in the last 12 months.

One possible reason breach history remains high is the lack of information on the location and classification of data. In this year's survey, only 16% of respondents said they have complete knowledge of where their data is stored, with only 23% of respondents being able to fully classify data. Safe harbor from breach notification processes also remains elusive, as 62% of those breached were unable to obtain it. In comparison, 61% of all U.S. respondents could not obtain safe harbor from encryption or tokenization.

## Breaches Reported by APAC Respondents

**Q: HAS YOUR ORGANIZATION  
EVER BEEN BREACHED?**



Base: APAC respondents (n=876)

Source: 451 Research's 2022 Data Threat custom survey

# 32%

of APAC respondents reported that they had experienced a security breach in the last 12 months.

Only

# 16%

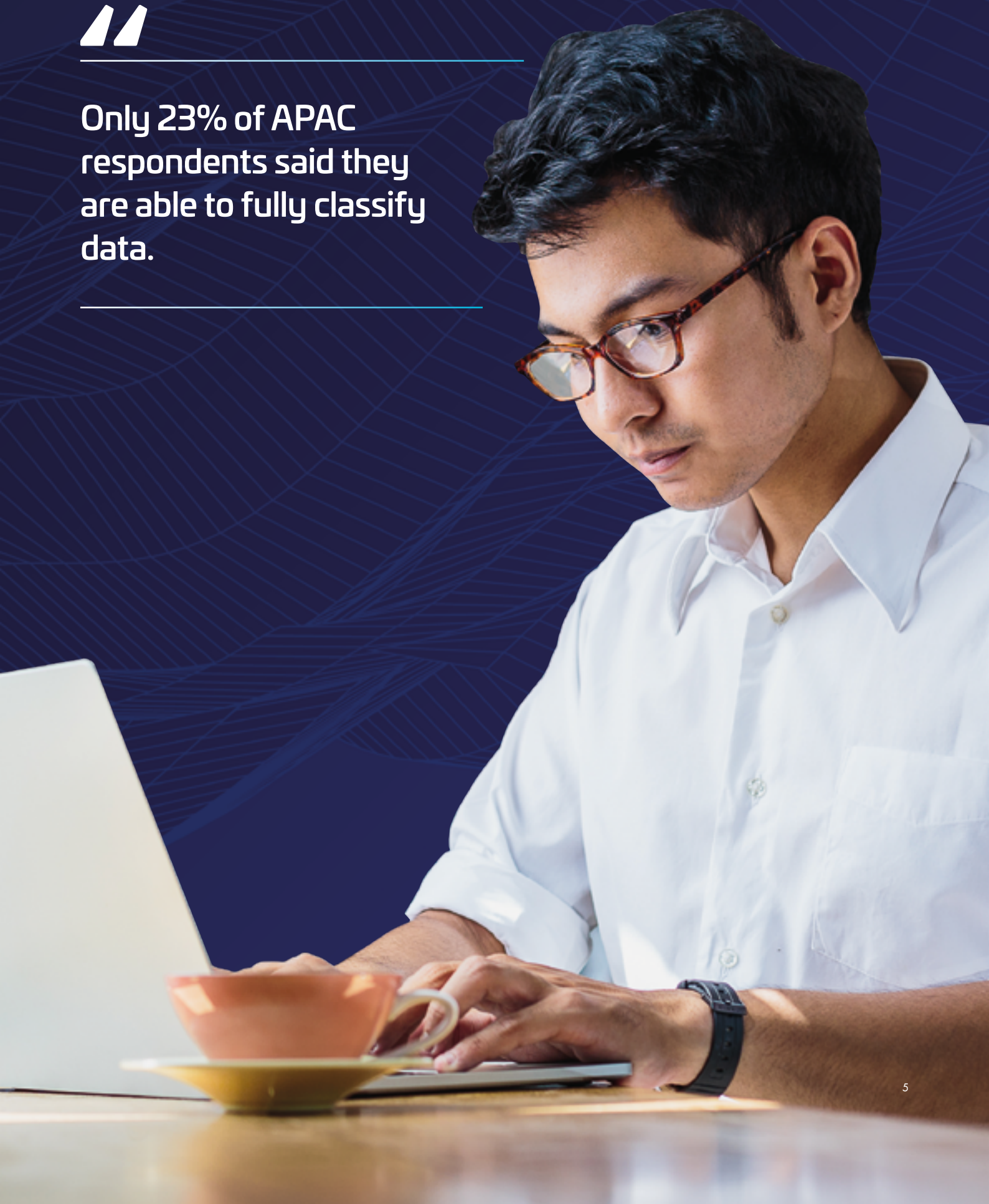
of APAC respondents said they had complete knowledge of where their data is stored.

“

---

Only 23% of APAC  
respondents said they  
are able to fully classify  
data.

---





## Security Threats

Forty-five percent of respondents reported an increase in the number of attacks. Of those respondents who saw an increase, 58% saw an increase in ransomware attacks, 57% saw an increase in malware attacks and 45% saw an increase in denial-of-service attacks. Among last year's respondents, 57% ranked malware as the leading source of increased security attacks, with ransomware coming in second at 47%. The speed with which ransomware attacks occur and the increased economic impact will continue to alter the way organizations detect and respond to breaches.

Despite increased attacks, organizations remained confident. Seventy-seven percent of respondents said they would trust their organization with their own personal data. For all worldwide respondents, trust in their own organizations remained high at 79% overall.

Among threat actors in ranked choice voting, 75% of APAC respondents prioritized internal, incidental error, followed by 73% who prioritized external adversaries motivated by ideology – “hacktivists.” External adversaries with geopolitical goals, such as nation-state actors, came in third place at 69%. In another ranked choice vote, 34% of respondents said that their cloud storage was the greatest target for adversaries. Cloud databases and on-premises web applications were prioritized as targets by 31% and 28% of respondents, respectively.

## Ransomware Planning and Response

In 2022, the study had a new focus on ransomware planning and response. The speed and severity of ransomware, compared to “low and slow” data exfiltration attacks from most malware, impacts both data confidentiality and availability. Twenty-four percent of APAC respondents reported that they had suffered a ransomware attack. Of those attacked, 82% had some internal or external impact, and 24% suffered a significant internal or external impact. Twenty-one percent of respondents said they paid or would pay the ransom to recover from an attack. Of greater concern, only 47% of respondents said they have a formal ransomware response plan that they would follow. Given the severity and speed of ransomware attacks, a centralized formal plan that ties together diverse stakeholders such as security operations, legal and senior leadership teams should be first when coordinating a coherent response.

Only

# 47%

of respondents said they have a formal ransomware response plan that they would follow.





# Continued Era of Remote Working

Many organizations extended remote working for employees in the past year. Concerns about security risks of remote employees continued in 2022, with 33% “very concerned” and 47% “somewhat concerned.” It was much the same story worldwide: 31% of global respondents said they were “very concerned” and 48% “somewhat concerned.” Attitudes improved regarding current remote access security solutions to effectively enable employees to securely work: 24% of respondents said they were “highly confident,” 34% said “significantly confident,” 26% said “slightly confident” and 16% said “not at all confident” in their secure remote access solutions.

When asked about remotely accessing applications, 59% of APAC respondents said they use virtual desktop infrastructure (VDI). VPN and cloud-based single sign-on (SSO) tied for second place at 53%, with zero-trust network access (ZTNA) at 38%. By comparison, worldwide numbers were 59% for VPN, 55% for VDI, 51% for cloud-based SSO and 36% for ZTNA.



**In 2022, 80% of APAC respondents were either “very concerned” or “somewhat concerned” about security risks of remote employees.**

# Zero Trust Strategies Gaining Momentum

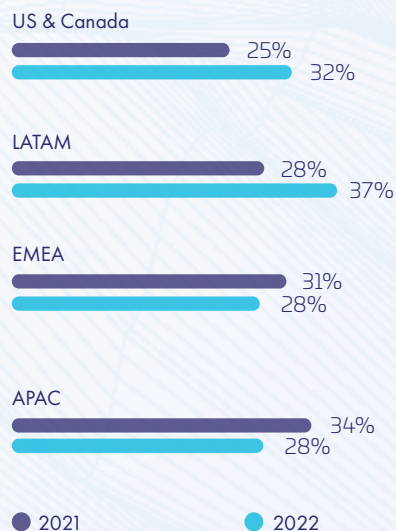
The principle of zero trust is based on the recognition that identities, networks, devices, applications and data are no longer confined within traditional corporate networks. In general, zero-trust principles mean that there are no implicit or assumed levels of trust between identities, networks or even sets of data. As such, perimeter-based approaches to security that rely on outdated notions of “trust” that are largely rooted in physical location (i.e., which network data exists on) have become less effective. In contrast, zero-trust approaches rely primarily on identity as a central means of granting access to resources.

Perhaps because zero-trust security strategies cover so much ground, fewer respondents said they have a formal zero-trust strategy. In 2021, 34% of respondents reported having a formal strategy, while in 2022, only 28% said they have embraced a formal strategy. At the time of this study, another 28% of respondents were still in research and planning to develop a formal zero-trust security strategy.

Forty-eight percent of respondents said they relied on “some concepts” of zero-trust to shape their overall cloud security strategy, and another 30% of respondents said that zero trust shaped their cloud security strategy to a “great” extent. These figures are slightly lower than worldwide results. Among all global respondents, 47% said they rely on “some concepts” of zero trust and another 34% said zero trust shapes their cloud security strategy to a “great” extent.

## Formal Zero-Trust Strategy/Policy Among Respondents

### WHERE ARE YOU ON YOUR ZERO TRUST JOURNEY?



Base: All respondents (2,800; displaying percentage who selected “Execution: We have a formal strategy and are actively embracing zero-trust policy”)

Source: 451 Research’s 2021 and 2022 Data Threat custom survey



**In 2022, APAC respondents that said they had a formal zero-trust security strategy was down by 6% against 2021.**



# Cloud Momentum, Cloud Coverage Gaps

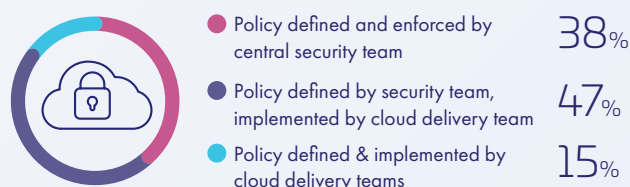
Organizations worldwide place increasing amounts of data in the cloud, and APAC organizations are no exception. In 2021, 31% of respondents stated that 41%-50% of their data was stored in external clouds, and 25% said more than 50% of their data was stored in external clouds. In this year's survey, 51% of respondents said they have at least 40% of their data in external clouds, and 19% reported more than 60% of their data is in the cloud. Worldwide, 55% of respondents said they have at least 40% of their data in the cloud, and 23% said they have at least 60% in the cloud.

The gaps in protection are shrinking. In 2021, only 30% of respondents said 41%-50% of their sensitive data stored in the cloud was encrypted, and only 17% of respondents said that more than 50% of their sensitive cloud data was encrypted. In 2022, 48% of respondents said at least 40% of their sensitive cloud data is encrypted, and 21% said at least 60% of their sensitive cloud data is encrypted. Recent breach history remains high but is improving. In 2021, 37% of respondents experienced a breach or failed an audit involving cloud data and applications in the last 12 months. In 2022, this improved to 33% of respondents.

Despite growth in the cloud and cloud-first strategies, last year, 46% of respondents "agreed" or "strongly agreed" that it was more complex to manage privacy and data protection regulations in a cloud environment compared to on-premises networks within their organization. In 2022, 51% of respondents said that they "agreed" or "strongly agreed" that cloud privacy and data protection regulations are more complex to manage than on-premises environments. Worldwide respondents in 2022 reported the same, as 51% "agreed" or "strongly agreed." Adding to some of this complexity, different personas enforce cloud security strategy. In 2022, 47% of APAC respondents said that policies are centrally defined by a security team, but defining technical standards and enforcing them is up to the individual developer or application owner. Another 38% said that policies and standards are centrally defined and enforced by the security team.

## Policy Definition and Implementation Stakeholders

### HOW DO YOU DECIDE AND ENFORCE POLICIES FOR CLOUD SECURITY?




Base: APAC respondents (n=876)

Source: 451 Research's 2022 Data Threat custom survey

# 33%

of APAC respondents said they experienced a breach or failed an audit for cloud applications or cloud data in the last 12 months.

# Most Firms Are Using a Multicloud Strategy

A woman with long dark hair wearing a black hijab and a light pink button-down shirt is shown in profile, looking towards the right. Her hands are on a laptop keyboard. The background is a solid light blue.

The status of encryption in the cloud is further complicated by the fact that the majority of organizations in our survey use multiple cloud providers across all “flavors” of cloud: IaaS, PaaS and SaaS. In 2022, we found closer parity among APAC respondents employing AWS and those using Azure: 49% use AWS and 43% use Azure for production workloads. This is a significant change compared to 2021, when 53% of respondents used AWS and only 46% used Microsoft Azure. The most varied cloud usage, unsurprisingly, is with SaaS. The greatest percentage of APAC respondents (31%) use more than 50 SaaS applications, and 16% use more than 100 SaaS apps. A small proportion (3%) reported using more than 500 SaaS apps. As more SaaS is delivered in API form, the expected heterogeneity of cloud usage is increasing concerns (and challenges) about managing encryption keys and identities across multiple providers.



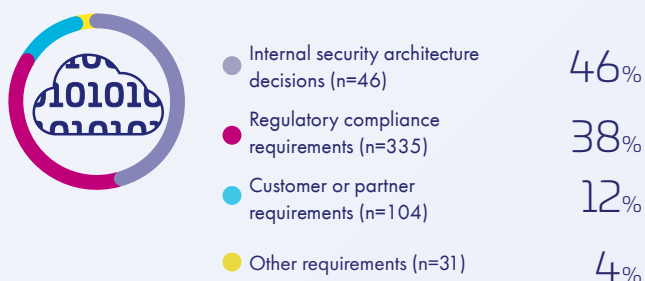
# Multiple Clouds and Key Management Options Driving Complexity

Given the diversity of IaaS and SaaS, existing on-premises infrastructures, as well as security mandates requiring consistent controls throughout agencies, it's no wonder that organizations have a mixture of encryption and key management solutions. Specifically, our 2022 survey found that the largest percentage (39%) of APAC-based organizations employ between five and seven separate key management products, while a smaller number (11%) have as many as 8-10 key management products. These typically include a mix of key management software, hardware security modules, homegrown solutions and spreadsheets or flat files.

Organizations not only have a variety of cloud providers and key management technologies to choose from, but they can also choose the types of controls for encryption and key management from cloud providers. To illustrate, more than half (59%) of respondents indicated that their cloud provider controls most or all of their encryption keys, and another 34% said their organization controls most or all of the encryption keys deployed for cloud data. Only 7% of APAC respondents in 2022 reported a 'shared' key generation/key control arrangement, where the company controls key-generation material, but the cloud provider furnishes key control.

## Cloud Encryption Drivers

**Q: WHAT IS THE PRIMARY DRIVER FOR DECISIONS ON WHERE AND HOW ENCRYPTION IS USED IN CLOUD?**



Base: APAC respondents (n=876)

Source: 451 Research's 2022 Data Threat custom survey

Many cloud services and platforms may offer data encryption as a feature, yet underlying key management is not as well-emphasized or understood, which may add further complexity to cloud data protection. When asked what security technologies prioritized sensitive data in the cloud, 61% of respondents chose data-at-rest encryption, followed by 53% for multi-factor authentication. Key management was in third place at 51%. Organizations would be better served taking a holistic look at the different encryption and key management solutions to identify further gaps in implementation and safety.

# 39%

of APAC-based organizations employ between five and seven separate key management products.

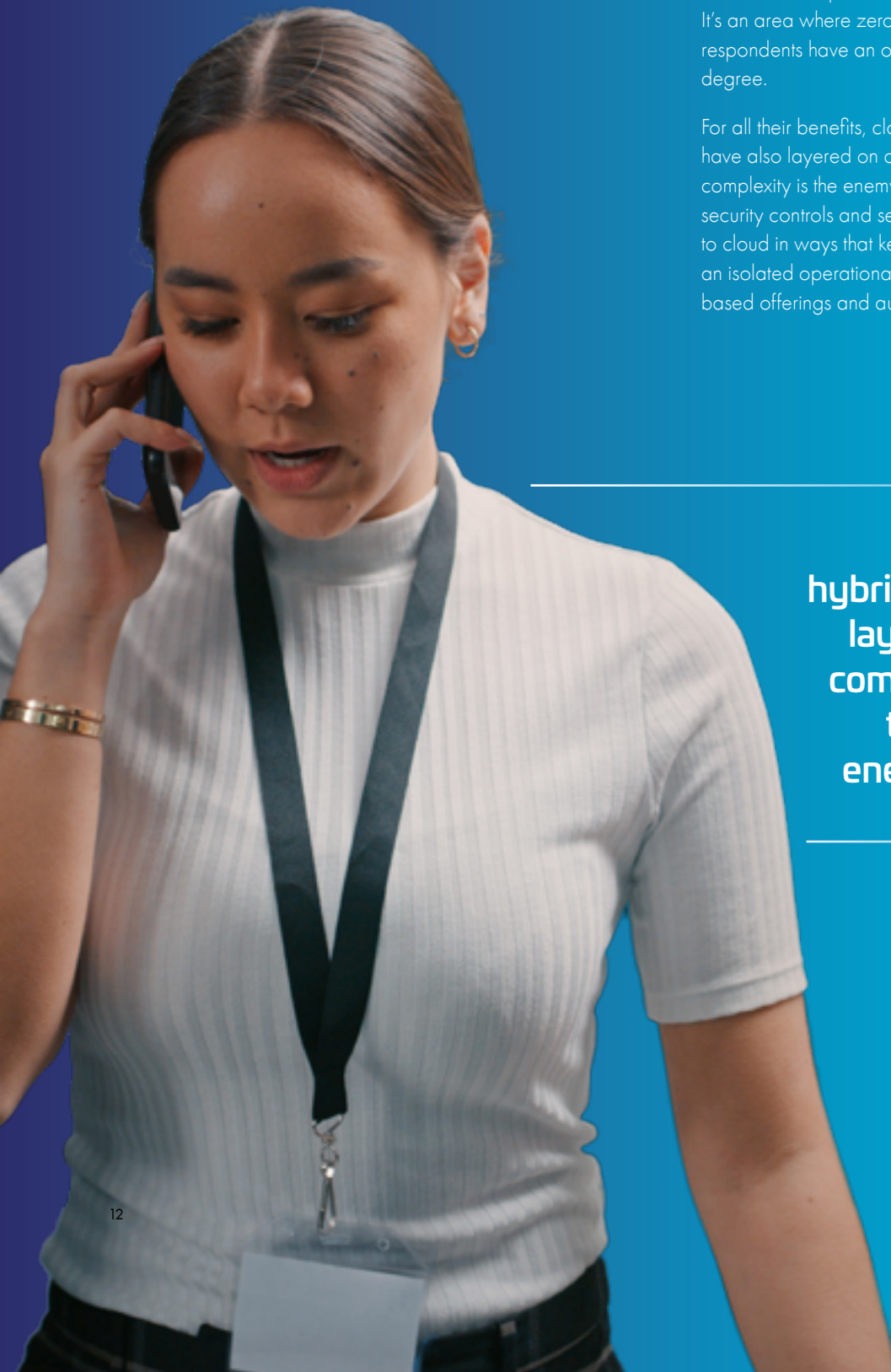
# Moving Ahead

This study can serve as an indicator of potential paths that organizations in the APAC region may choose to follow on their security journey. One of the key lessons learned from the pandemic was that security strategies must be sufficiently agile to respond to a rapidly changing world, but also flexible enough to deal with the hybrid nature of our infrastructure, applications, data and users as both work-from-home and cloud become permanent fixtures in the security landscape. It's an area where zero-trust approaches can help, and APAC respondents have an opportunity to leverage this to a greater degree.

For all their benefits, cloud computing and hybrid environments have also layered on considerable complexity – and complexity is the enemy of good security. This means that both security controls and security management will need to extend to cloud in ways that keep each cloud environment from being an isolated operational realm, as well as leverage service-based offerings and automation to reduce manual burdens.



**Cloud computing and hybrid environments have layered on considerable complexity and we know that complexity is the enemy of good security.**





# About This Study

The COVID-19 pandemic has had an immediate and dramatic impact on IT teams around the globe, and its long-term effects are still evolving. The APAC edition of the 2022 Thales Data Threat Report study looked at various aspects of those impacts in a wide-ranging survey of security professionals and executive leadership that touched on issues ranging from COVID-19 and work-from-home strategies to quantum computing. The 2022 Thales Data Threat Report is based on a survey of almost 2,800 security professionals and executive leaders, including 876 respondents from the APAC region.



## Industry Sector

Manufacturing1	57	Consumer Products1	07
Retail	154	Computers/ Electronics/Software1	06
Technology	127	Engineering1	04
Financial Services1	20	Federal Government1	03
Healthcare	115		
Public Sector1	09		

## 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



## Contact us

For all office locations and contact information,  
please visit [cpl.thalesgroup.com/contact-us](https://cpl.thalesgroup.com/contact-us)

**[cpl.thalesgroup.com/data-threat-report](https://cpl.thalesgroup.com/data-threat-report)**

