THALES
Building a future we can all trust

EUROPE AND MIDDLE EAST EDITION

2023 CLOUD SECURITY STUDY

The Challenges of Data Security and Sovereignty in a Multicloud World

#2023CloudSecurityStudy

cpl.thalesgroup.com

Introduction

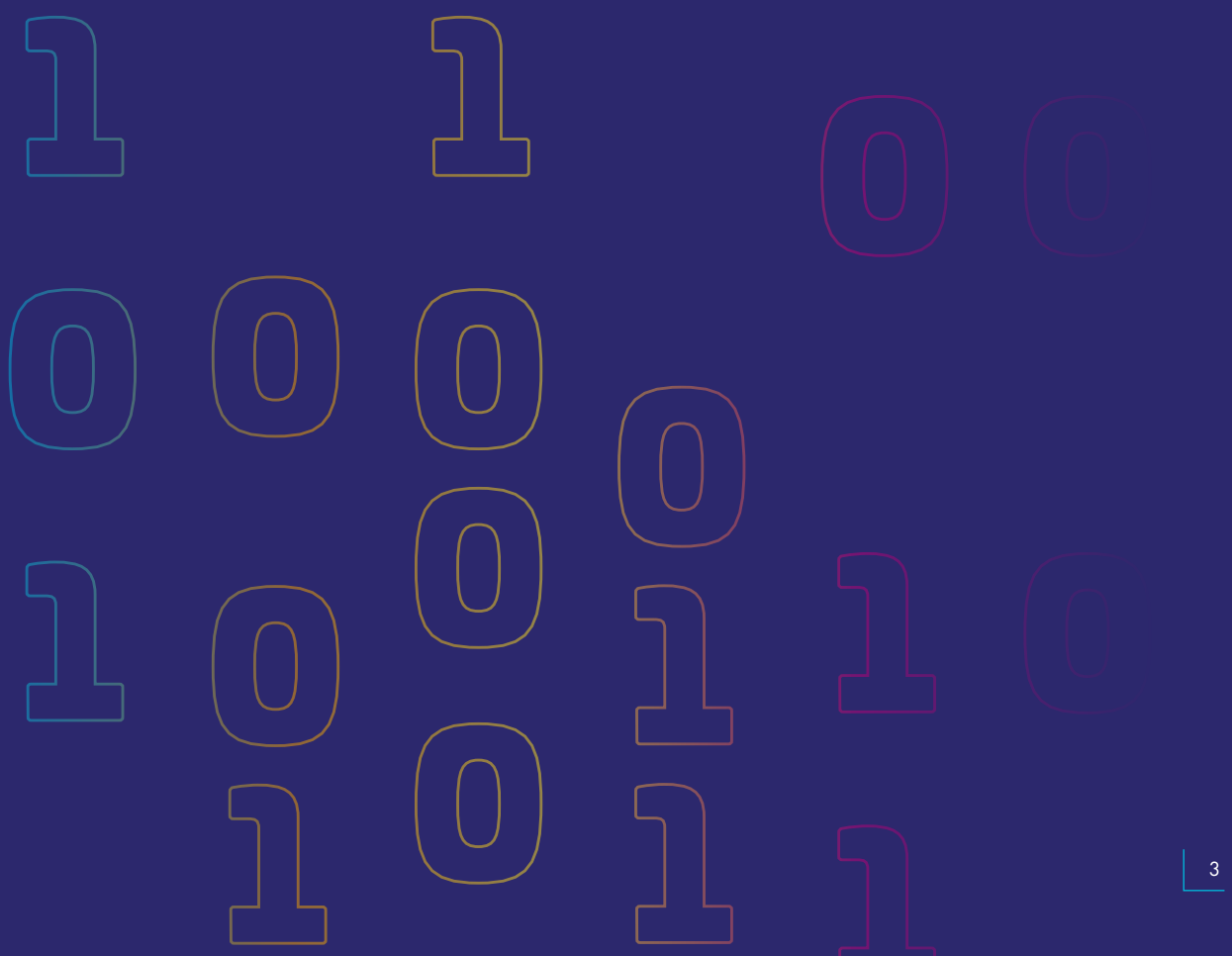
In this report, we share key findings from the 2023 Thales Cloud Security Study, focusing on results specific to the Europe and Middle East (EME) region. EME, like the rest of the world, has become cloud-first and multicloud. As a result, the majority of IT security professionals report that it is now even more complex to secure the cloud. The latest edition, based on a survey of 1,180 respondents in seven EME markets, explores the challenges of security in cloud environments that have become a critical element in modern digital infrastructure and services. Unsurprisingly, many of the results from the EME region are close to the global responses, but we call out key differences as applicable.

S&P Global
Market Intelligence

Source: 2023 Cloud Security custom survey from S&P Global Market Intelligence, commissioned by Thales.

Sponsored by

Contents



Key findings

SaaS application usage is EXPANDING

Cloud storage and SaaS apps are top-cited targets for attacks.

103

EME respondents report an average of 103 SaaS apps in use — a 45% increase over last year — increasing the number of points where data must be secured.

23%

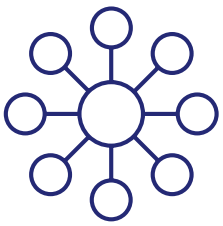
Moreover, in 2021, 14% of EME respondents reported that their enterprises were using 51-100 SaaS applications. That number increases to 23% for 2023 respondents, a 64% increase, 6 percentage points higher than the global increase.

30%

EME respondents identify cloud-delivered SaaS as the leading target for attackers (cited by 30%), followed closely by cloud-based storage (28%).

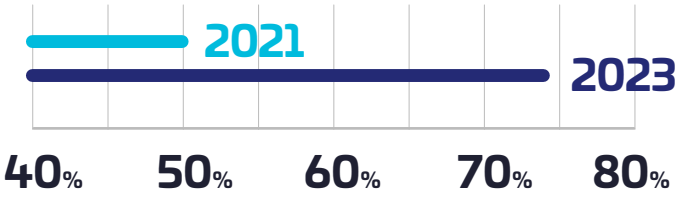
45%

growth reported in average number of SaaS applications used in EME.

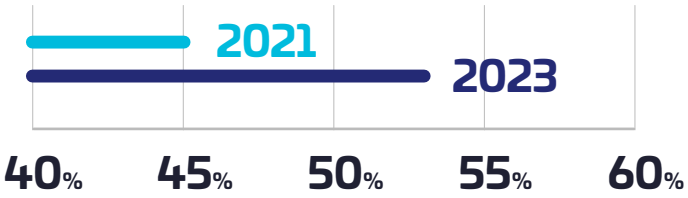


Securing cloud data is becoming more complex.

The proportion of EME respondents who report that more than 40% of their data in the cloud is sensitive has risen from 50% in 2021 to 74% this year.



The percentage of EME respondents who agree that securing data in the cloud is more complex than securing it on-premises has increased to 53% from 45% two years ago — very close to the global response.



ONLY 20%

The results also suggest that a greater proportion of sensitive data needs to be encrypted — only 20% of EME respondents report that more than 60% of their sensitive cloud data is encrypted, similar to the worldwide result. EME respondents, on average, report that 45% of their sensitive cloud data is encrypted.

We're only human:

Human error is the top reported cause of cloud data breaches.

59%

Well ahead of exploitation of vulnerabilities (17%), the second-most-common response. These are similar to the global results of 55% and 21%, respectively.

Encryption key management complexity is a serious issue.

EME respondents report using multiple key management systems;

64%

say they have five or more key management systems in place.

ONLY 14%

say that they control all their encryption keys in cloud environments, identical to the worldwide figure.

Multicloud is today's reality.

On average, EME respondent organisations are using 2.2 cloud infrastructure providers, similar to the global results. More than three-quarters (79%) have more than one cloud provider.

Digital sovereignty issues loom large on multiple fronts.

Respondents report high usage of cloud-provider-dependent encryption key management systems and growing concerns about sovereignty mandates.

82%

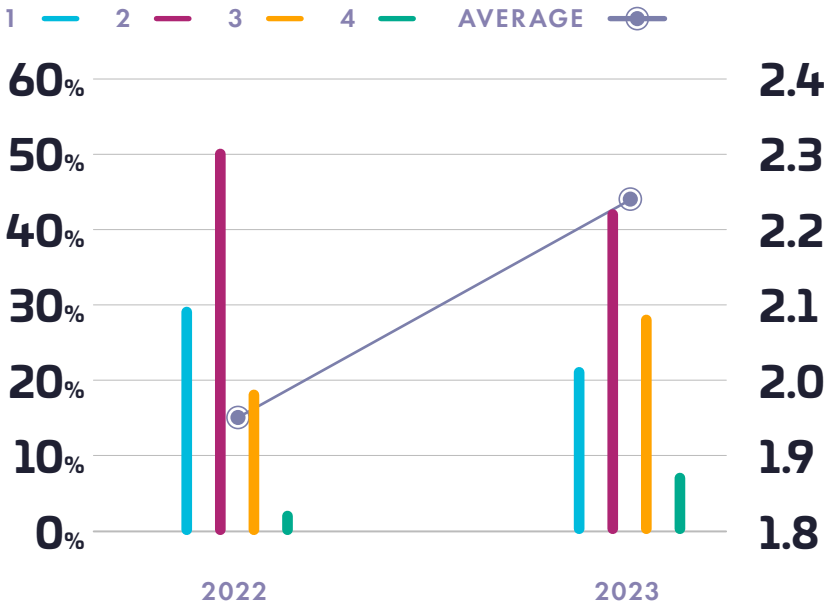
of EME respondents express concern about the impact of digital sovereignty issues on cloud deployments, similar to the global figure.

It's a multicloud world

Multicloud use continues to grow. On average, EME respondents are using 2.24 cloud infrastructure (IaaS and PaaS) providers, up 15% from 1.95 a year ago. A majority of respondents (53%) note that they find it more complex to secure data in the cloud compared to on-premises, and the growing number of cloud providers could be driving that issue.

In EME, multicloud is the rule, not the exception

More organisations are reporting multiple cloud Infrastructure as a Service (IaaS) providers in use in production environments, pushing the distribution and resulting average higher.



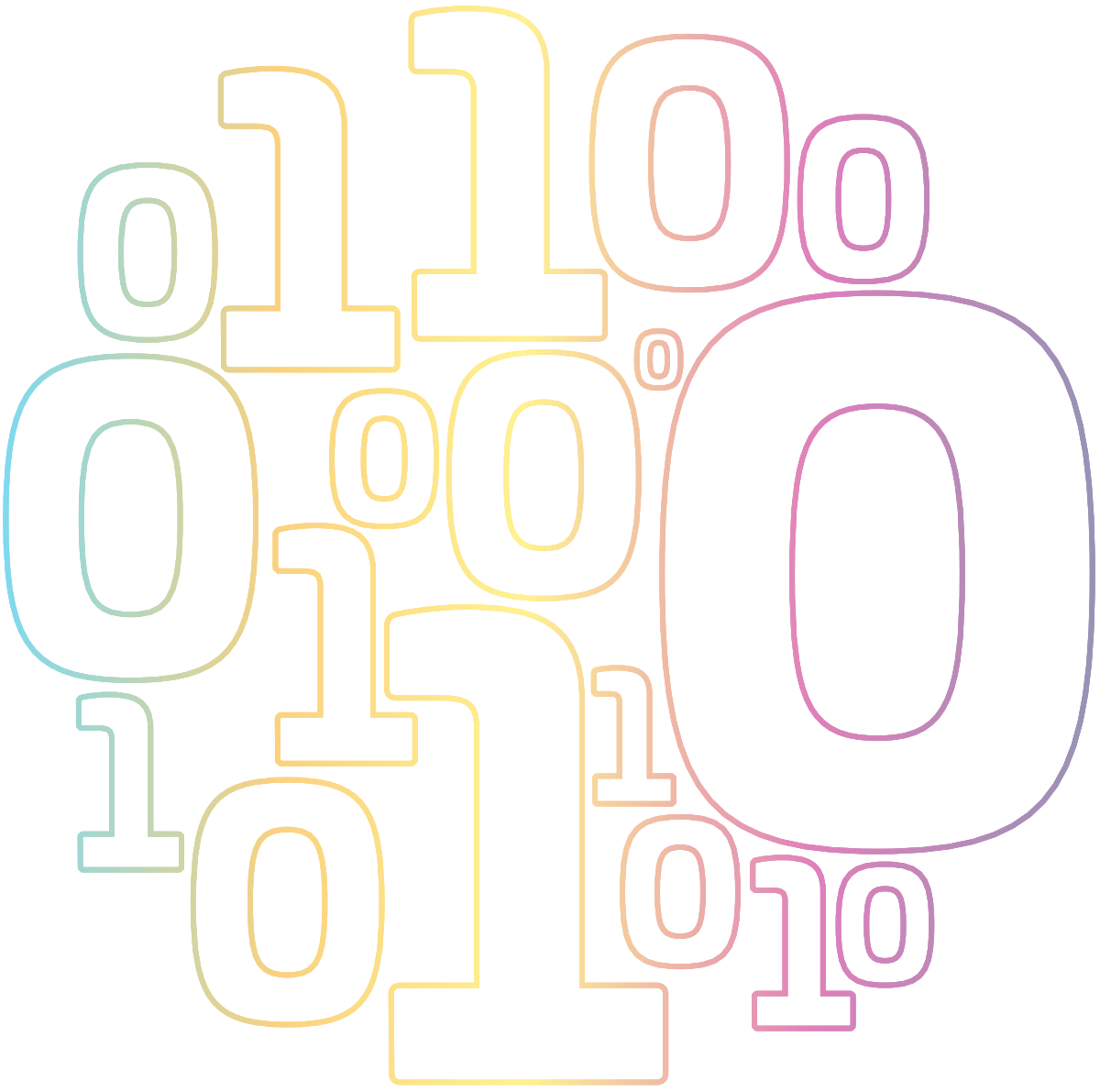
Source: S&P Global Market Intelligence's 2022-2023 Cloud Security custom surveys

15%

growth in the number of cloud IaaS/PaaS providers reported over the past year

The EME cloud threat landscape

Nearly one-third (30%) of EME respondents say cloud-delivered SaaS is the top target for cyberattacks, while 28% identify cloud storage. Just short of half (46%) say they have experienced a data breach in their cloud environment. However, the number experiencing a cloud data breach in the last year is down 7 percentage points (from 46% to 39%), encouraging news for the region.



Cloud data concerns

The average proportion of data in the cloud is rising in the EME region, moving from 23% to 28% (a 22% increase, 4 percentage points larger than the global increase), but the bigger story is the increasing proportion of sensitive data in the cloud. The share of EME organisations reporting that more than 40% of their data in the cloud is sensitive has risen from 57% in 2021 to 74% this year — a 30% increase. And while more sensitive data is being encrypted, it's still not enough. Only 59% of EME respondents report that more than 40% of their sensitive data in the cloud is encrypted, identical to the worldwide number. EME respondents, on average, report that 45% of their sensitive cloud data is encrypted, in line with the worldwide number. This may be due to difficulties in managing and deploying encryption across multiple cloud providers.

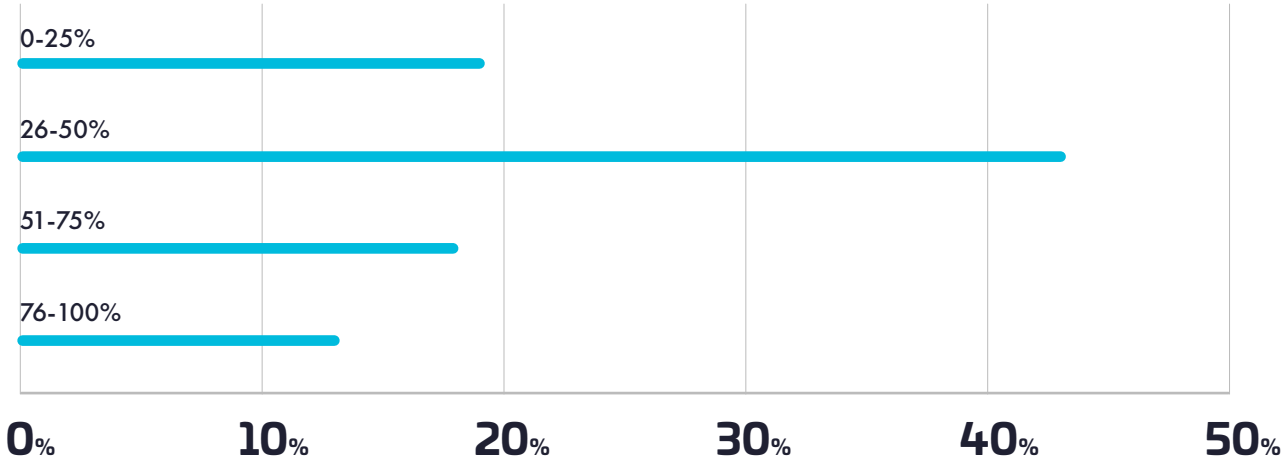
ONLY

59%

of EME respondents indicate that more than 40% of their sensitive data in the cloud is encrypted.

EME respondents, on average, report that 45% of sensitive cloud data is encrypted, equal to the global result

What percentage of your organisation's sensitive data in the cloud is encrypted?



Source: S&P Global Market Intelligence's 2023 Cloud Security custom survey

Impacts of digital sovereignty

Digital sovereignty is an emerging strategic initiative, and privacy compliance represents opportunities for enterprises to accelerate their digital transformation. Four-fifths (82%) of EME respondents say they are "somewhat" or "very" concerned about the impact of digital sovereignty on cloud deployments, very close to the global result. Nearly all EME respondents (95%) say that designating or changing the location and jurisdiction of data or implementing full data encryption are acceptable measures to achieve various levels of digital sovereignty, close to the global figure. More than a third (36%) believe that location is important for all of their workloads, similar to the worldwide result.

Operational complexity in the cloud

More than half of EME respondents (53%) indicate that it is more complex to manage data protection and privacy in the cloud than in on-premises environments, close to the worldwide figure. Only 14% of respondents say that they control all encryption keys in their cloud environments, identical to the global response. Nearly two-thirds (64%) say they have five or more key management systems, 2 percentage points higher than worldwide (62%). Although the EME figure is slightly higher than worldwide, it still indicates that more work is needed to simplify key management.

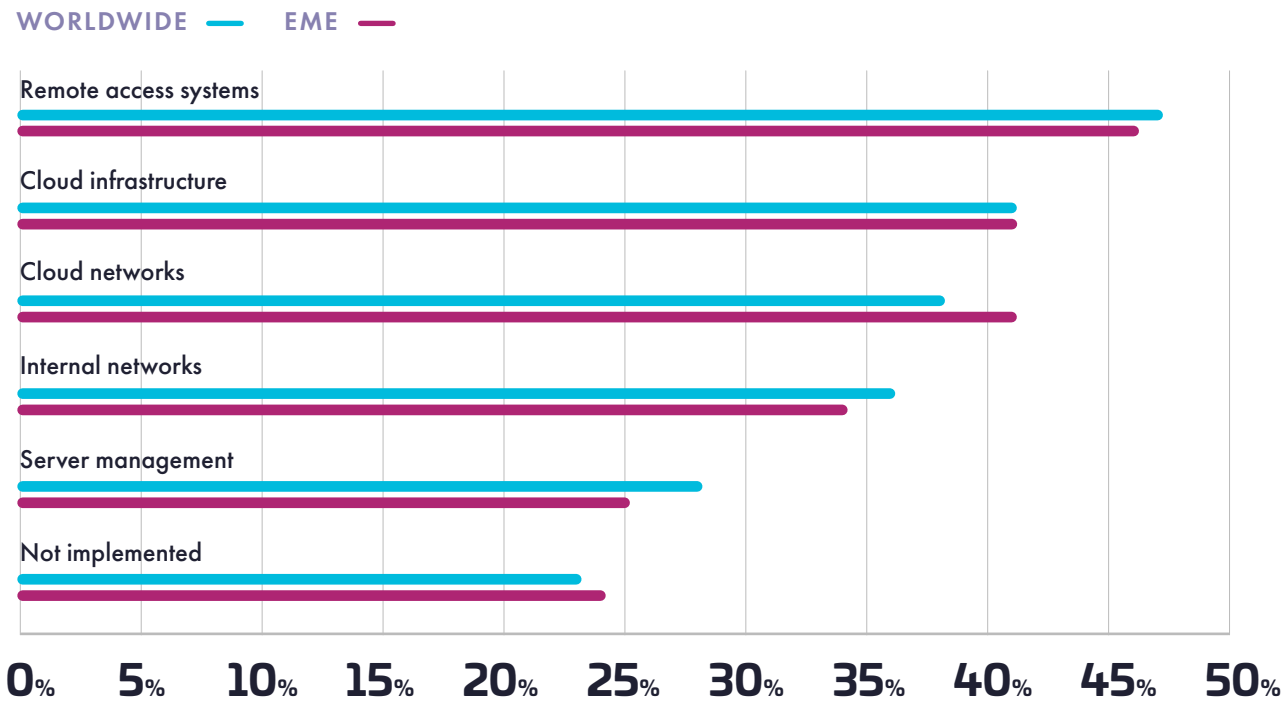
Pathways to better cloud security

Identity and access management has been identified as a top mitigating control for data breaches. Strong MFA adoption has increased to 67% among EMA respondents, 2 percentage points higher than the worldwide figure, but more is needed. Simplifying encryption management is another change needed to increase overall cloud security. In a multicloud world, organisations must centrally manage keys for use across their infrastructure — on-premises as well as in the cloud.

Getting to a zero-trust posture in the cloud can build a better foundation for operational security. Only 41% of EME respondents have zero-trust controls on cloud infrastructure, and the same proportion (41%) use zero-trust controls in cloud networks, similar to the global results.

Zero trust use in EME and worldwide

How does your organisation use zero trust practices?



Source: S&P Global Market Intelligence's 2023 Cloud Security custom survey

Moving ahead

Organisations are operating in a multicloud world, and they need effective and efficient ways to secure their data within it. Data protection in the cloud must become simpler to manage to overcome issues with human error and misconfiguration. The most effective way to improve cloud security is to ensure that cloud environments can be treated as an extension of existing infrastructure and not a special case.

The study results point to the challenges that EME organisations are facing in securing data in cloud environments. EME respondents are accelerating the shift to multicloud infrastructure, and they need to be able to secure that infrastructure effectively and efficiently. They need to overcome the complexity of working across cloud infrastructure and SaaS environments. Data protection in the cloud must become simpler to manage to overcome issues with human error and misconfiguration. The results of the study indicate the following specific areas that need improvement:

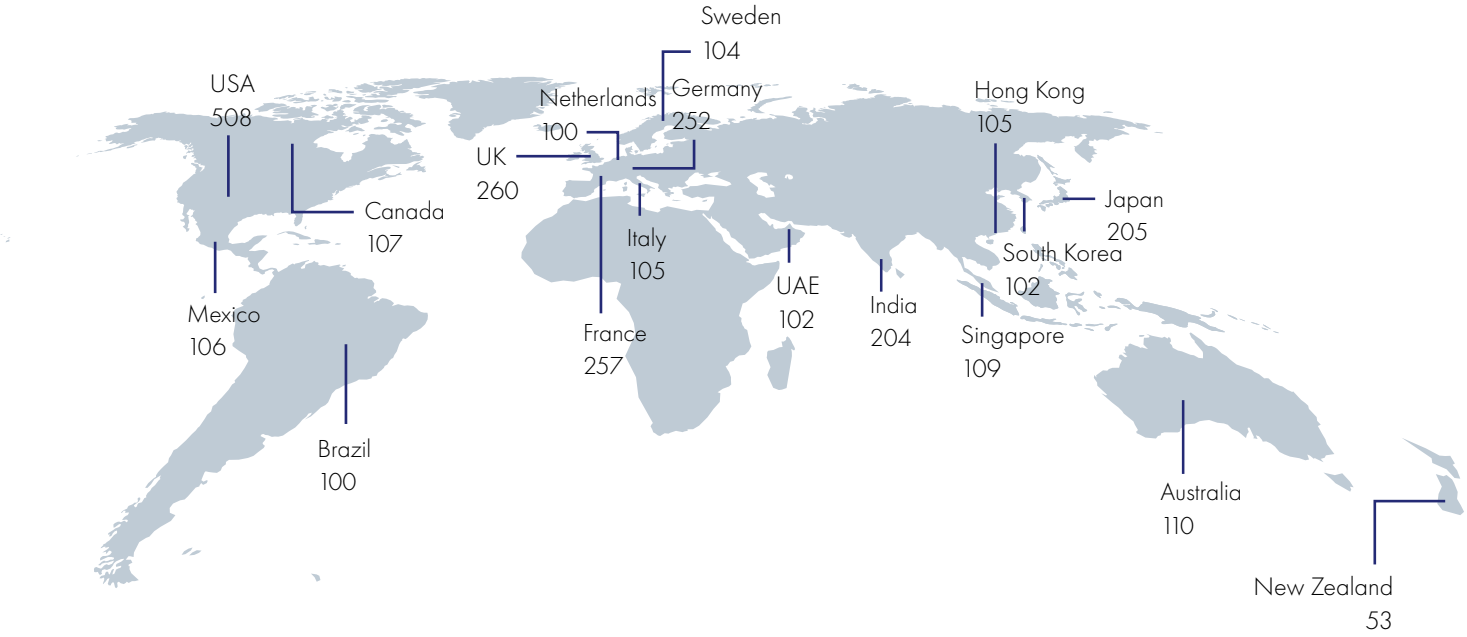
- **Key management consolidation.**
- **Greater use of data encryption.**
- **Gaining control of encryption keys.**
- **Achieving great efficiency through security automation.**

EME respondents, on average, report using more key management environments than global respondents, raising concerns about increased complexity. By consolidating, they can deliver the operational control that is needed to scale up the use of encryption in ways that existing security teams can handle. At the same time, organisations need to take advantage of the force-multiplying power of automation. Automation is underutilised in security when compared to other technical disciplines, and in addition to the increased efficiency that it provides, it is another tool to reduce the risk of human error. These improvements can also bolster digital sovereignty compliance efforts with the necessary controls to ensure that data resides where it should and that it is well-protected.

The most effective way to improve cloud data security is to ensure that cloud environments can be treated as an extension of existing infrastructure, not a special case. The greater use of multicloud and SaaS in the region requires technologies that can span the multiple environments that organisations inhabit with a common security management environment. It's a pathway to making all of an organisation's data protections more effective and efficient.

About this study

This research was based on a global survey of 2,889 respondents that was fielded in November and December 2022 via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about the level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated an affiliation with organizations with annual revenue of less than US$100 million and with US$100 million-$250 million in selected countries. This research was conducted as an observational study and makes no causal claims. Data from the worldwide study was extracted to focus on the 1,180 respondents across seven key EME markets (France, Germany, Italy, Netherlands, Sweden, United Arab Emirates and the United Kingdom).

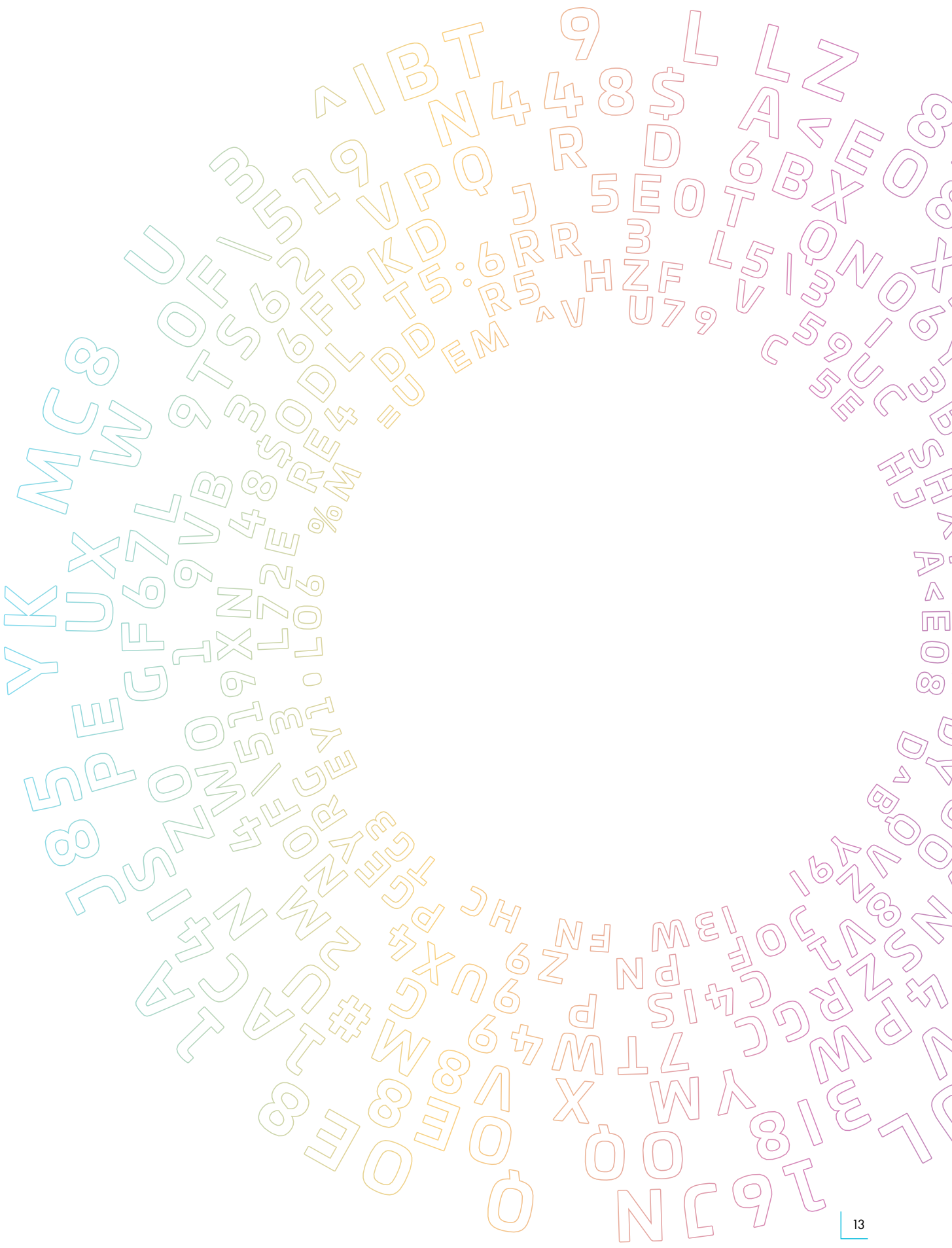


Revenue

$100m to $249.9m	**91**
$250m to $499.9m	**749**
$500m to $749.9m	**796**
$750m to $999.9m	**748**
$1Bn to $1.49Bn	**229**
$1.5Bn to $1.99Bn	**134**
$2Bn or more	**142**

Industry Sector

Retail	**158**
Manufacturing	**148**
Financial services	**140**
Healthcare	**139**
Federal government	**125**
Public sector	**122**
Technology	**117**
Automotive	**114**
Pharmaceuticals	**108**
Telecommunications	**101**



THALES

Building a future we can all trust

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

cpl.thalesgroup.com/cloud-security-research