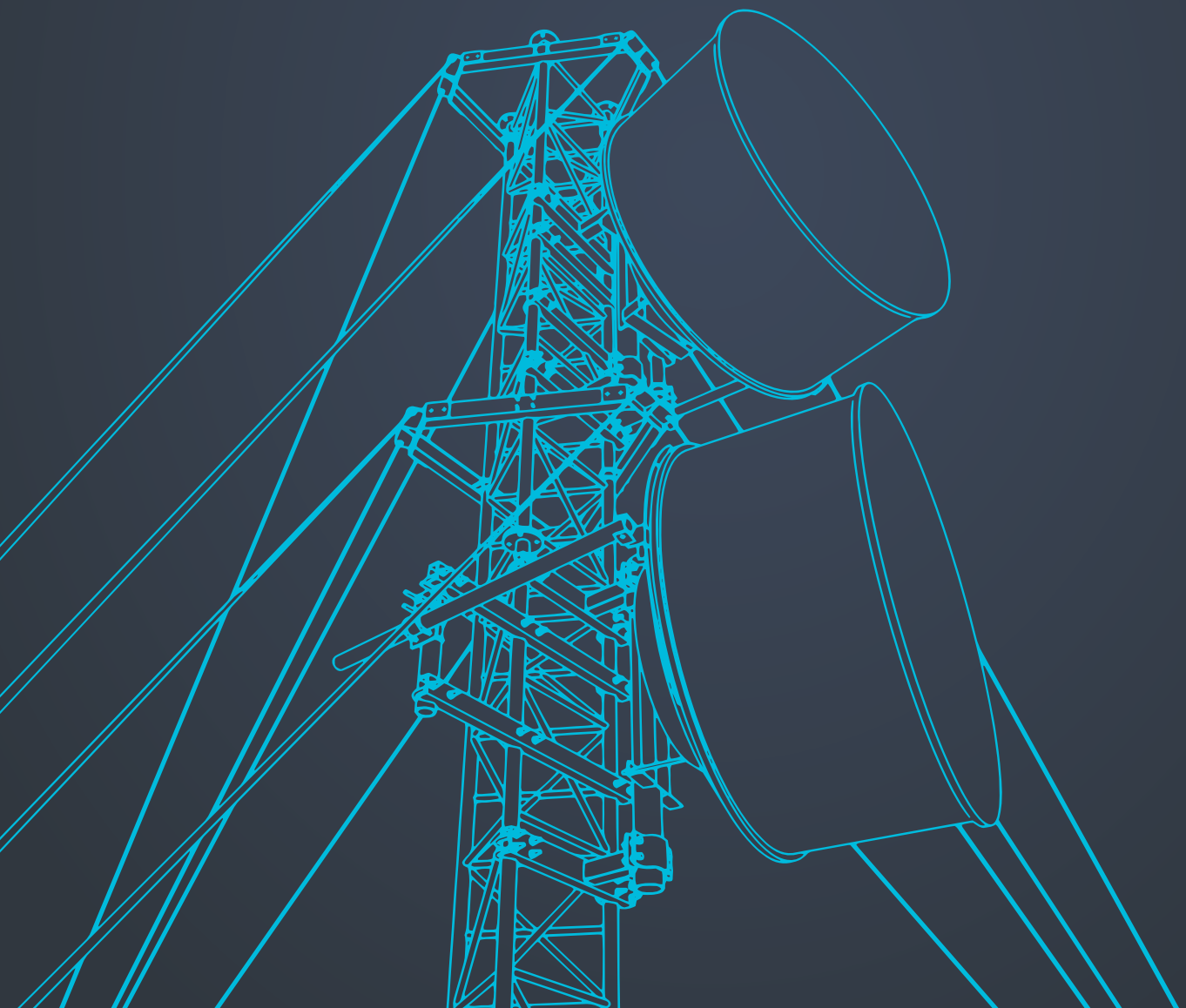
THALES
Building a future we can all trust

TELECOMMUNICATIONS EDITION

2023 DATA THREAT REPORT

Cybersecurity Challenges in the 5G Era



Introduction

Telecommunications firms have always faced a unique set of security challenges, and the rapid shift to higher levels of digitization means they have much more data to protect. They have to secure their environments with infrastructure that has become more multicloud and more complex. The latest edition of the report explores the perspectives of more than 100 telecom respondents in 18 countries regarding the threat landscape, challenges and strategies for data protection in the context of 5G, and infrastructure areas such as cloud.

S&P Global
Market Intelligence

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

Contents

Key findings

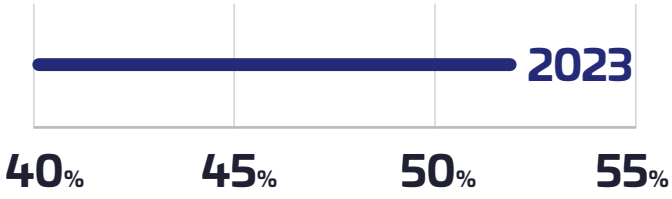
5G security is a significant concern in telecom and in the broad market.

81%

of telecom respondents are concerned about 5G security threats

Securing data in cloud is considered complex

but the percentage who deem cloud security more complex than on-premises security has decreased slightly to 53% from 58% last year.



Concerns about the impact of quantum computing are higher in telecom than in the broader survey population.

Concerns about quantum-related decryption risks for data (59%) and networks (69%) outpace overall survey results by 4 percentage points and 7 percentage points, respectively.

Human error is the most commonly identified security threat

87%

identify it as a threat, and a third (33%) rank it as the top threat.

There needs to be **greater encryption** of **sensitive data.**

ONLY **1%**

of respondents have more than 90% of their sensitive data encrypted.

Digital sovereignty issues loom large on multiple fronts.

Many respondents report using cloud-provider-dependent encryption management, and a growing number express concerns about sovereignty mandates.

75% are concerned about the impact of digital sovereignty on cloud deployments.

Identity and encryption management complexity can be serious issues.

57%

of telecom respondents are using five or more encryption key management systems.

ONLY 42%

have deployed strong authentication (such as MFA) for their internal, non-IT employees.

Multicloud is today's reality:

Telecom respondents on average are using 2.36 cloud infrastructure providers. Most (80%) have two or more cloud providers.

113

The average number of SaaS apps used by telecoms

Telecom respondents on average are using 113 SaaS apps, 16% higher than the mean of 97 for the full survey population. This represents another increase in the number of points where data must be secured.

Cloud-based resources and SaaS applications are identified as the leading targets of attackers.

IoT devices are also an area of elevated concern among telecom respondents.

5G concerns

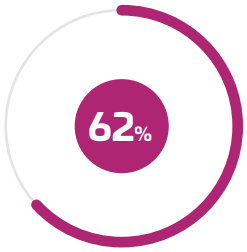
There is greater risk in any new technology, and although 5G deployments have been underway for a number of years, organizations are still developing a full understanding of the security implications. In telecom, there is risk not only in owned infrastructure, but also from third-party devices that are connected to the network. This presents an additional security challenge.

The telecom industry has a larger set of security issues than other enterprises. Identity and access management extends from telecom companies' internal resources out to subscribers, and the operational data on which they run their businesses is a notable target for fraud. Understandably, telecom respondents (81%) are more likely to express concern about 5G security risks compared to the broader survey population (77%). Moreover, telecom companies must address the 5G-related concerns of the broader market as telecom players implement 5G technology to enable businesses across all industries.

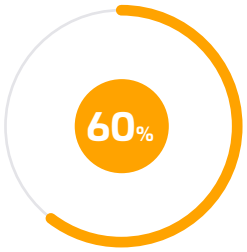
5G security concerns

What aspects of 5G security are you most concerned about?

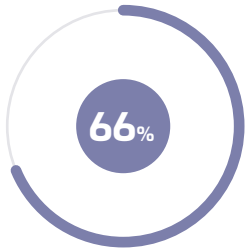
Protecting the identities of devices, people and things connected to 5G networks



Data that moves across 5G networks



Applications and infrastructure connected to networks



Increased attack surface in 5G

Source: S&P Global Market Intelligence's 2023 Data Threat custom survey.

The concerns of the telecom sector extend to their expectations regarding attack potential. Telecom businesses not only have to secure their internal environments, but they must also address risks posed to and by the users and devices that connect to telecom networks. Telecom respondents cite cloud-based assets as the leading concern for their internal environments. Cloud-based databases and storage systems are two of the top three reported attack targets, with SaaS applications taking the second spot.

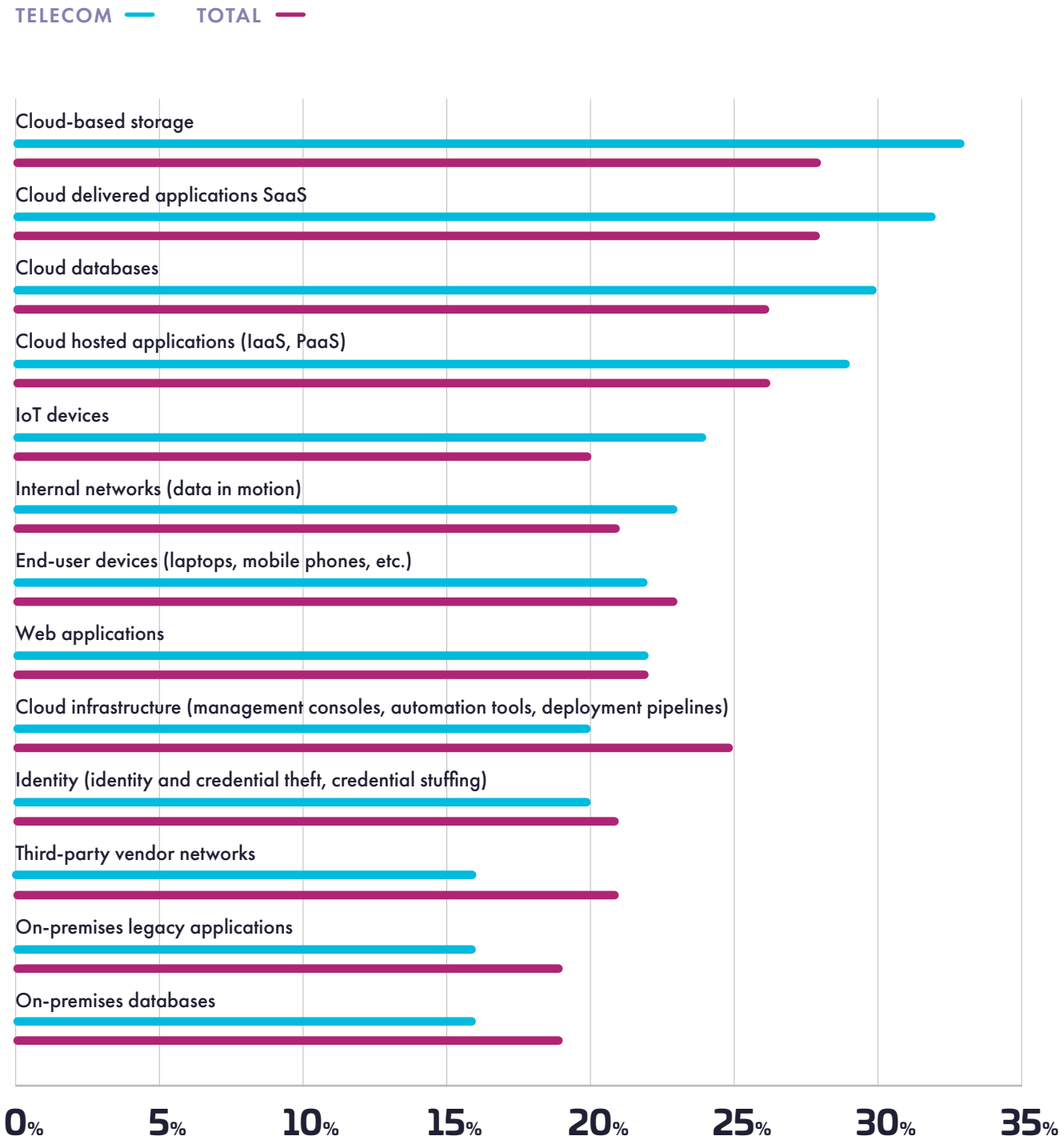
IoT devices also feature prominently among telecom respondents' concerns, ranking as the fifth-most-commonly cited target. Botnet recruitment and distributed denial-of-service (DDoS) attacks have historically targeted IoT devices. Broad market respondents are less concerned about IoT security risks, ranking IoT 11th out of 15 choices.

81%

of telecom respondents are concerned about 5G security risks, 4 percentage points higher than in the broader survey population (77%)

Biggest cyberattack targets

In general, which of the following are the biggest targets for cyberattacks?



Source: S&P Global Market Intelligence's 2023 Data Threat custom survey.

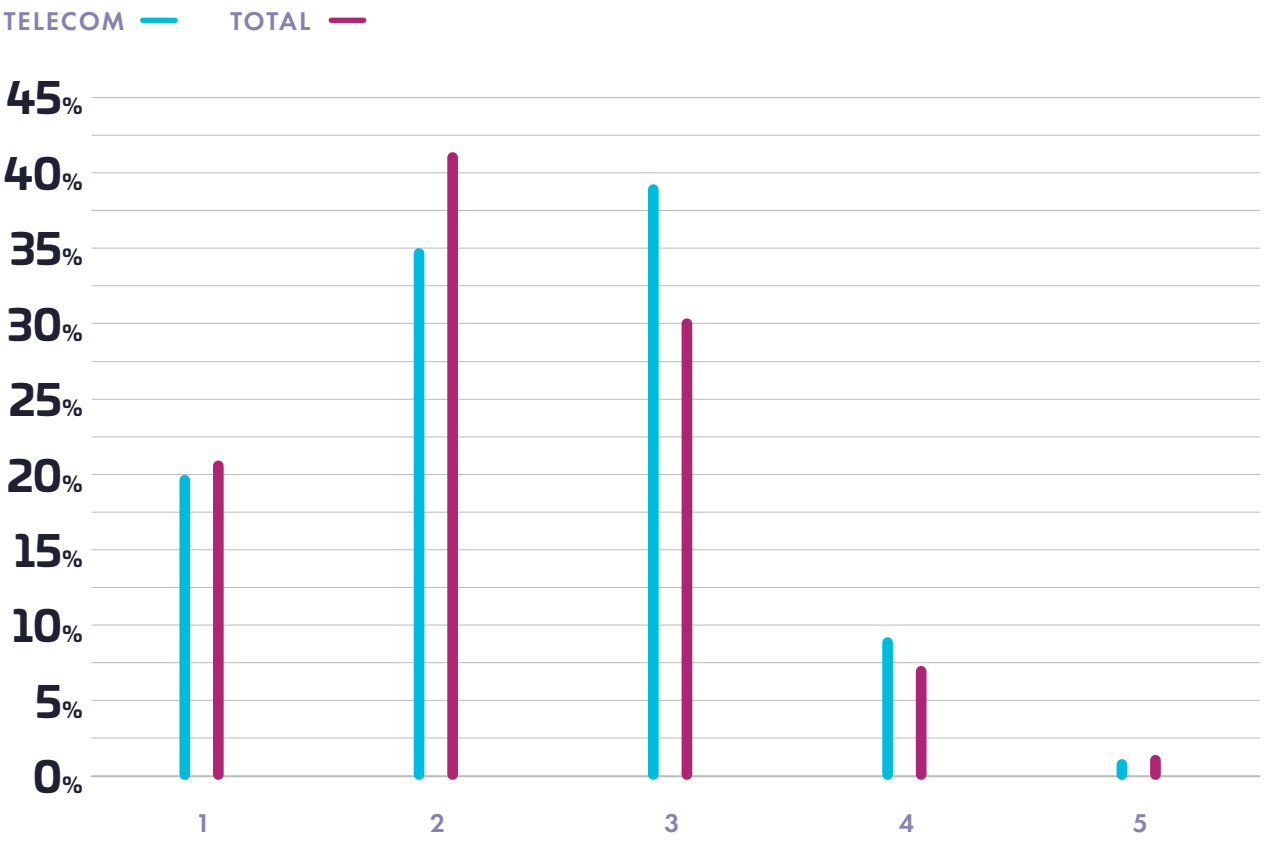
It's a multicloud world

Multicloud use among telecom companies is higher than in the broader survey population. The average number of cloud providers is 4% higher (2.36 versus 2.26). Larger numbers of providers can increase operational complexity and the risk of human error, which respondents identify as the leading cause of data breaches.

SaaS use is higher among telecom companies as well. While 15% of all respondents report that their enterprises use between 101 and 500 SaaS applications, that number increases to 22% of telecom respondents. Telecom companies report an average of 113 SaaS apps in use — 16% higher than the mean of 97 across the broad sample.

Number of cloud infrastructure providers

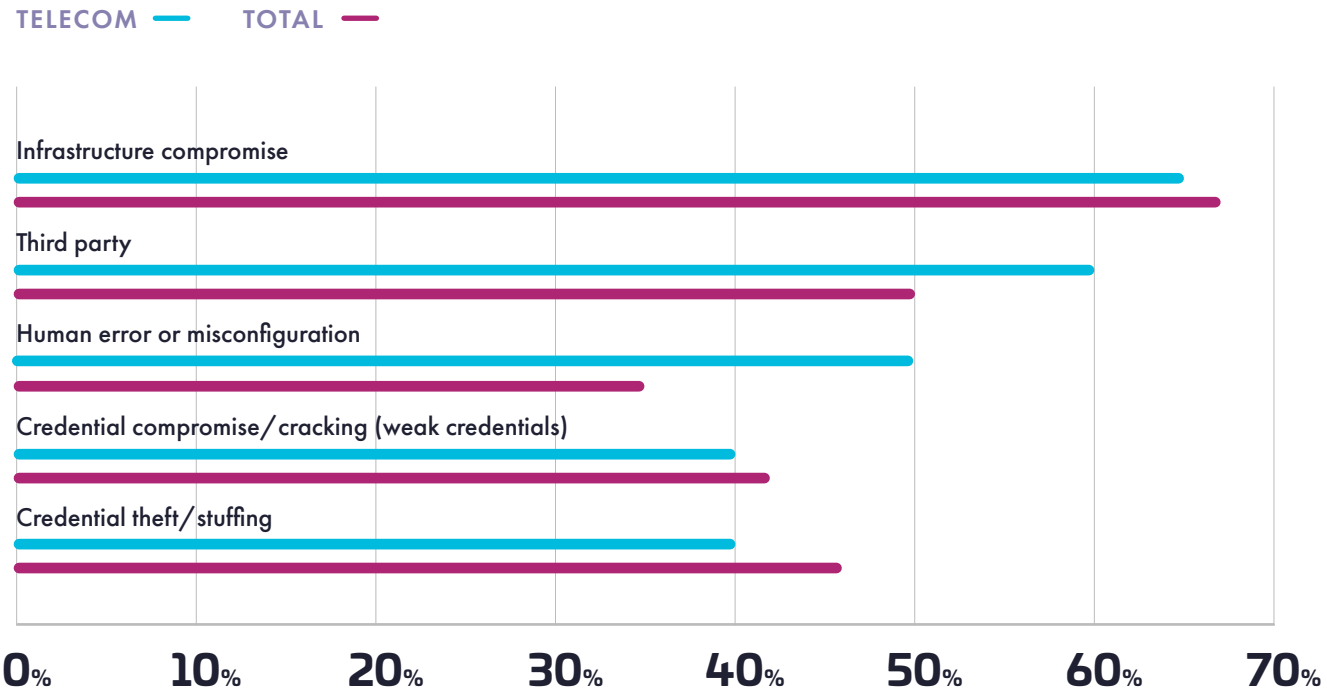
Of the following cloud Infrastructure as a Service (IaaS) providers, which does your organization use or plan to use in a production capacity?



Source: S&P Global Market Intelligence's 2023 Data Threat custom survey.

Types of cloud attacks increasing

What type of cloud infrastructure attacks are you seeing increase?



Source: S&P Global Market Intelligence's 2023 Data Threat custom survey.

The threat landscape for telecom

Telecom respondents report that cloud-based resources are the leading targets of attackers: cloud storage (33%), followed closely by SaaS apps, cloud databases and cloud hosted IaaS/PaaS. While infrastructure compromise is the most commonly reported type of cloud attack on the rise, human error figures much more prominently for telecom (50%) than for the total survey population (35%). This reflects the challenges that telecom companies face when operating at large scale and an understanding of the consequences of operational failures.

There is heightened concern among telecom respondents about the impact of quantum computing and its potential to break current encryption algorithms; 59% of telecom respondents express concern about quantum data decryption, versus 55% survey-wide, and 69% express concern about network decryption, versus 62% across all industries.

Nearly half of telecom respondents (44%) say they have experienced a data breach in their cloud environment. Among those that have experienced a cloud data breach, the percentage that experienced one in the last year is notably higher than among the broader survey population (57% versus 39%).

Data security concerns

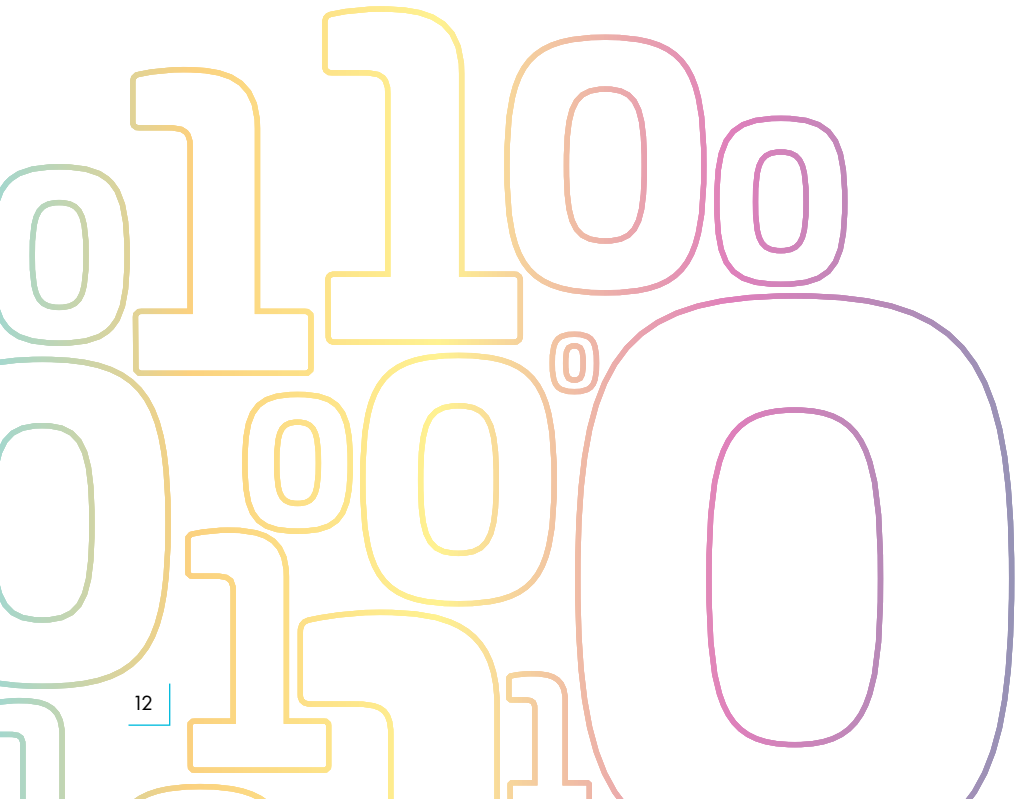
There is more data in cloud — the average reported proportion of organizational data residing in cloud has increased from 23% to 27% — but the bigger story has to do with sensitive data. The percentage of respondents who report that more than 40% of their cloud data is sensitive has increased from 49% in 2021 to 66% this year.

An increasing amount of sensitive data is being encrypted, but it's still not enough. Only 13% of respondents report that more than 60% of their cloud data is encrypted; on average, respondents say 45% of their cloud data is encrypted. Further complicating matters, only 24% of telecom companies report that they can classify all of their data, surprisingly 7 percentage points lower than the total survey population. The inability to classify data makes it much more difficult to effectively secure.

ONLY

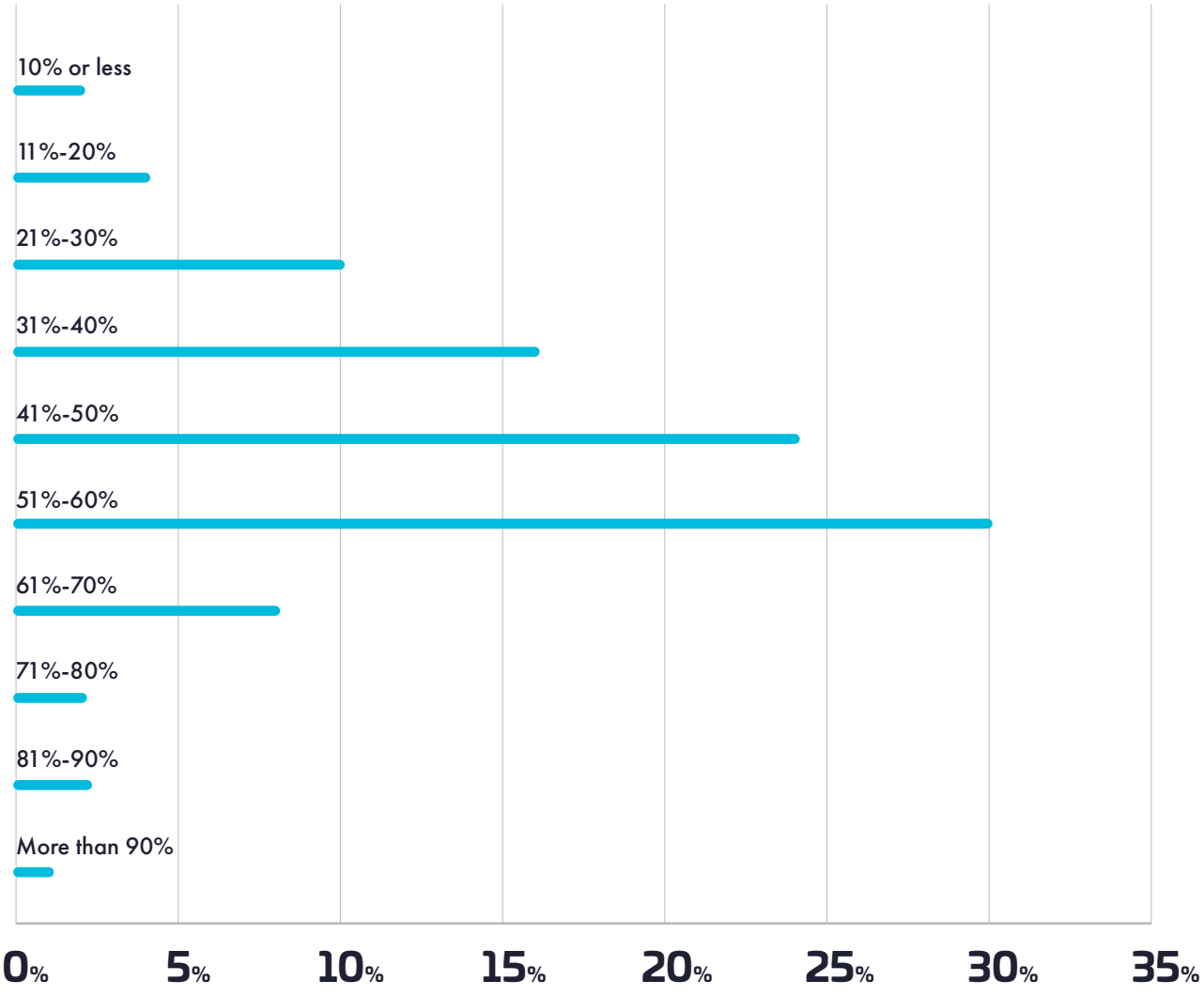
13%

of respondents report that more than 60% of their cloud data is encrypted.



Percentage of sensitive cloud data encrypted

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



Source: S&P Global Market Intelligence's 2023 Data Threat custom survey.

Impacts of data sovereignty

Digital sovereignty is an emerging strategic initiative and, along with privacy compliance efforts, represents an opportunity for enterprises to accelerate their digital transformation. When asked about digital sovereignty, 75% of telecom respondents say they are "somewhat" or "very" concerned about impacts on cloud deployments, lower than the broader market result of 83%. This may be because more telecom companies have already addressed these issues in their international operations.

Telecom companies face significant regulatory pressures, and nearly all telecom respondents (94%) 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. Telecom respondents are more likely to believe w location is important for all of their workloads, at 41% versus 35% of the total survey population.

94%

of telecoms say that designating the location and jurisdiction of data or implementing full data encryption are acceptable measures to achieve digital sovereignty

Operational complexity hampers security

More than half (53%) of telecom respondents indicate that it's more complex to manage data in cloud than in on-premises environments. Only 14% say they control all of their encryption keys in their cloud environments. More than half (57%) say they have five or more key management systems. This collision of concerns adds up to significant operational complexity for security teams as they work to protect data.

> **53% of telecom respondents say it is more complex to manage data in cloud than in on-premises environments."**

Pathways to better data security

Identity and access management has been identified as the top mitigating control for data breaches, but telecom companies are a long way from full deployment of more capable technologies. Adoption of strong authentication, such as MFA, has increased to 67%. While that's slightly better than the total survey population's 65%, it's still not good enough. For telecom companies, the second-most-common root cause of data breaches, after human error, is failure to secure privileged accounts with MFA (24%); failure to use MFA ranks dead last among root causes for the broad market, at 11%.

Simplifying encryption management is mandatory. In a multicloud world, organizations have to be able to centrally manage keys that are used across their infrastructure — on-premises, as well as in cloud.

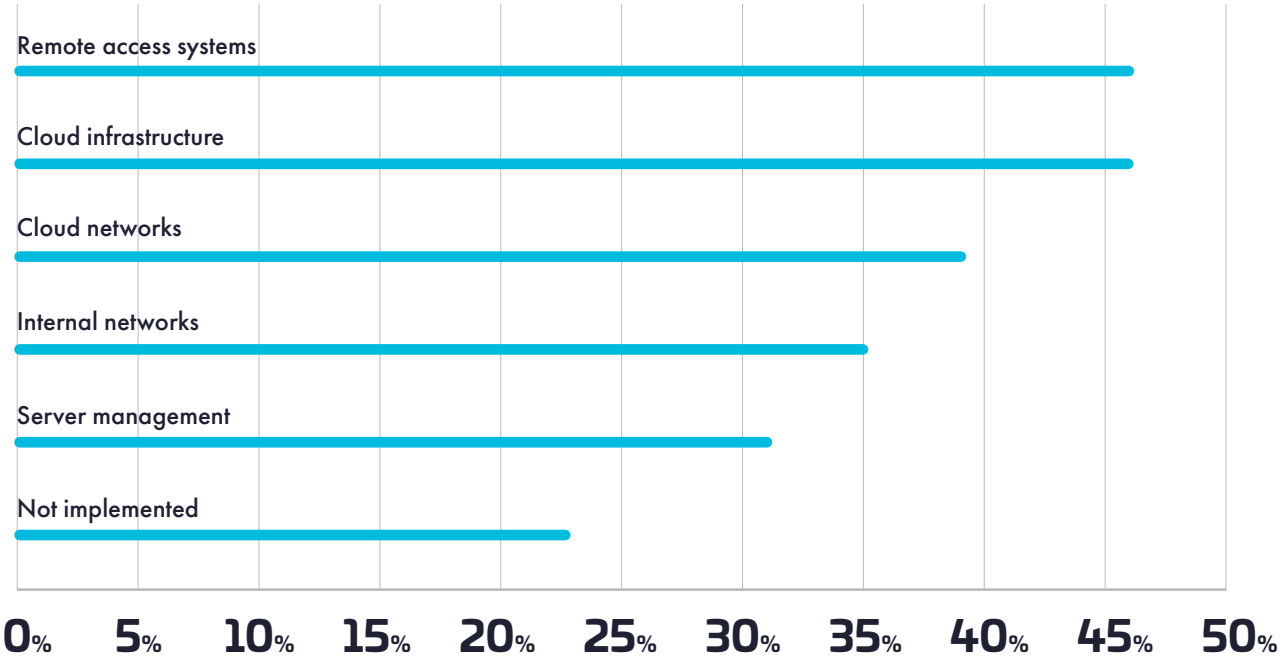
Getting to a zero-trust posture in cloud can build a better foundation for operational security. However, only 39% of telecom respondents report that they have zero-trust controls on cloud networks, and fewer than half (46%) use zero-trust controls in cloud infrastructure.

46%

fewer than half of telecoms use zero-trust controls in cloud infrastructure.

Implementation of zero-trust practices

How does your organization use zero-trust practices?



Source: S&P Global Market Intelligence's 2023 Data Threat custom survey.

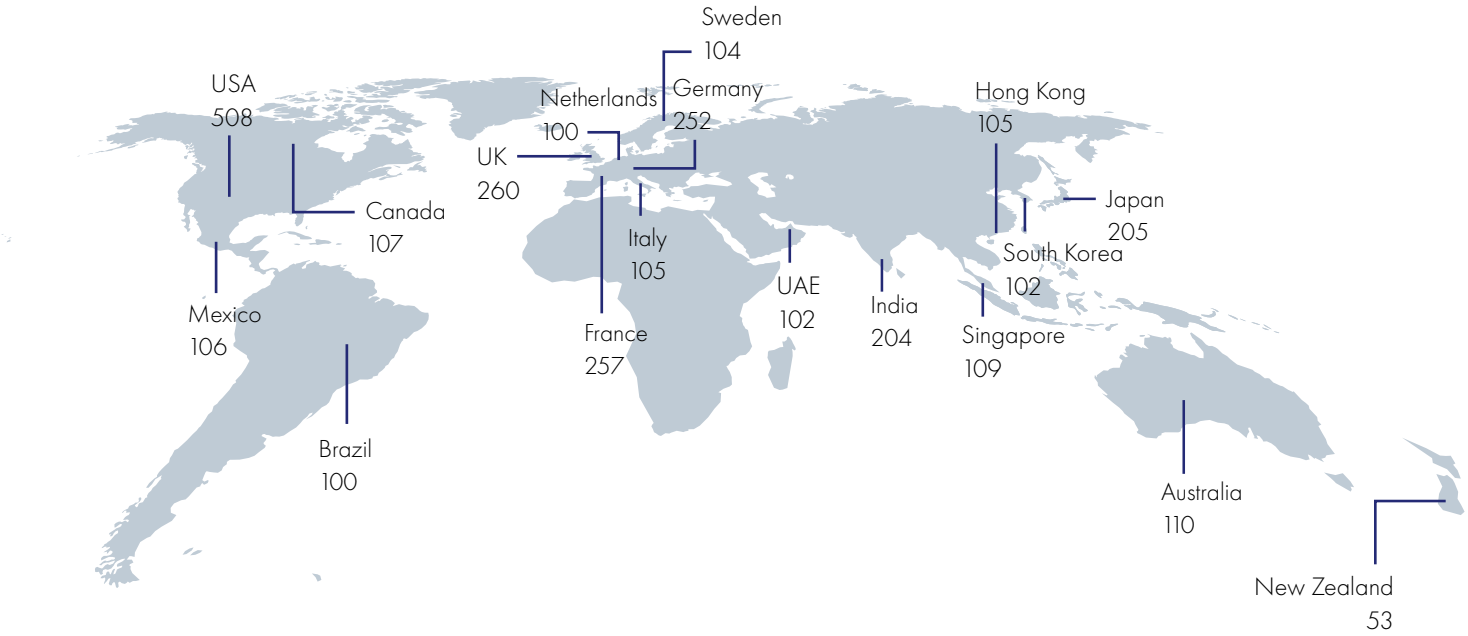
Moving ahead

Telecom companies face a unique set of risks and additional complexity in managing data security. The advent of greater 5G network capacity is a business opportunity, but it also brings a new set of risks. Those same networks are ever more critical to telecom customers as linchpins of their hybrid infrastructure. Telecom companies must not only secure their systems and data, but they must do so while also securing their customers in an environment that is a high-value target for attackers.

To deliver the security operations capabilities needed to achieve this, protection for sensitive data at rest and in motion have to become simpler to manage to overcome issues with human error and misconfiguration. At the same time, greater deployment of advanced IAM capabilities is needed to better secure data assets. Delivering effective and efficient security requires better automation and consolidated management. While there has been progress, there is still much more to do in the telecom sector.

About this study

This research was based on a global survey of 2,889 respondents of which 101 were telecommunications companies. The study 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.



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/telecom-data-threat-report