THALES
Building a future we can all trust

FINANCIAL SERVICES EDITION

2023 DATA THREAT REPORT

Securing Digital Markets

Introduction

The security challenges faced by financial services (FiServ) organizations cannot be overstated. As the managers and custodians of financial assets and related sensitive data, these organizations are under constant attack from bad actors and receive increasing scrutiny from regulators, while trying to address customer and competitive demands for greater digital access. Regulatory pressures can also constrain options in their digital transformation journey, which has contributed to a more cautious approach to cloud adoption than in some industries. Security teams in the FiServ industry need to secure infrastructure environments that have become more multicloud and more complex. There are positive trends in key areas, but still much work to be done. The latest Financial Services Edition of the Thales Data Threat Report explores the perspectives of 140 FiServ respondents in 18 countries regarding their understanding of the evolving security threat landscape, and challenges and strategies for protecting data, whether in the cloud, on-premises or across multicloud and hybrid environments.

S&P Global
Market Intelligence

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

Contents

Key findings 4

It's a multicloud world 6

The threat landscape for financial services 8

Data security concerns 10

Impacts of data sovereignty 12

Operational complexity hampers security 13

Pathways to better data security 14

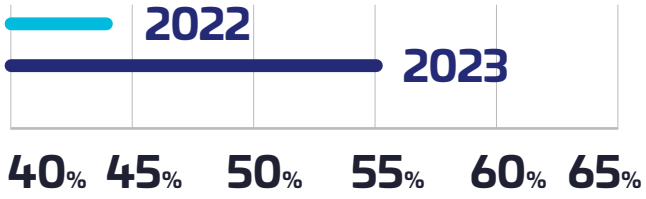
Moving ahead 16

About this study 17

Key findings

Securing data in cloud is considered complex

The proportion of FiServ respondents who agree with this sentiment has increased to 55% from 44% last year, a potential byproduct of increasing multicloud operations.



Identity and encryption management complexity can be serious issues

69%

of FiServ organizations surveyed have five or more key management systems.

71%

Stronger authentication is a priority in FiServ, indicated by higher levels of reported MFA deployment.

Multicloud is today's reality

particularly in FiServ, with the average number of cloud providers now exceeding two (2.16), growing 12% in the last year. Three-quarters of FiServ respondents (74%) have two or more cloud providers.

137

The average number of SaaS apps used by FiServ

FiServ respondents report greater use of SaaS applications, which increases the number of points where data must be secured. The average number of applications in use jumped 67% over three years, from 82 to 137.

Leading targets of attackers

34%

Cloud-hosted applications

31%

Cloud infrastructure

Ransomware is a greater concern for financial services

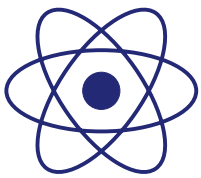
64%

compared to the total survey population. Nearly two-thirds of FiServ respondents (64%) report seeing an increase in attacks, versus 49% survey-wide. Notably, more FiServ respondents also report having experienced an attack (35% vs 22% overall).

Digital sovereignty issues loom large on multiple fronts

There is high reported use of cloud-provider-dependent encryption management, alongside growing concerns about sovereignty mandates.

79% are concerned about the impacts of sovereignty issues on cloud deployments.



FiServ organizations are more concerned than the broader survey population about some of the risks of quantum computing

Concerns about blockchain attacks (49%) and network decryption of sensitive data (66%) are both cited more frequently by FiServ professionals than by those in other industries.

Human error is a large concern for FiServ organizations in many areas

79% selected it and almost a third of those ranked it as their top threat (30%).

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

ONLY 46% of sensitive data in cloud is encrypted on average — more FiServ organizations control all of their own encryption keys.

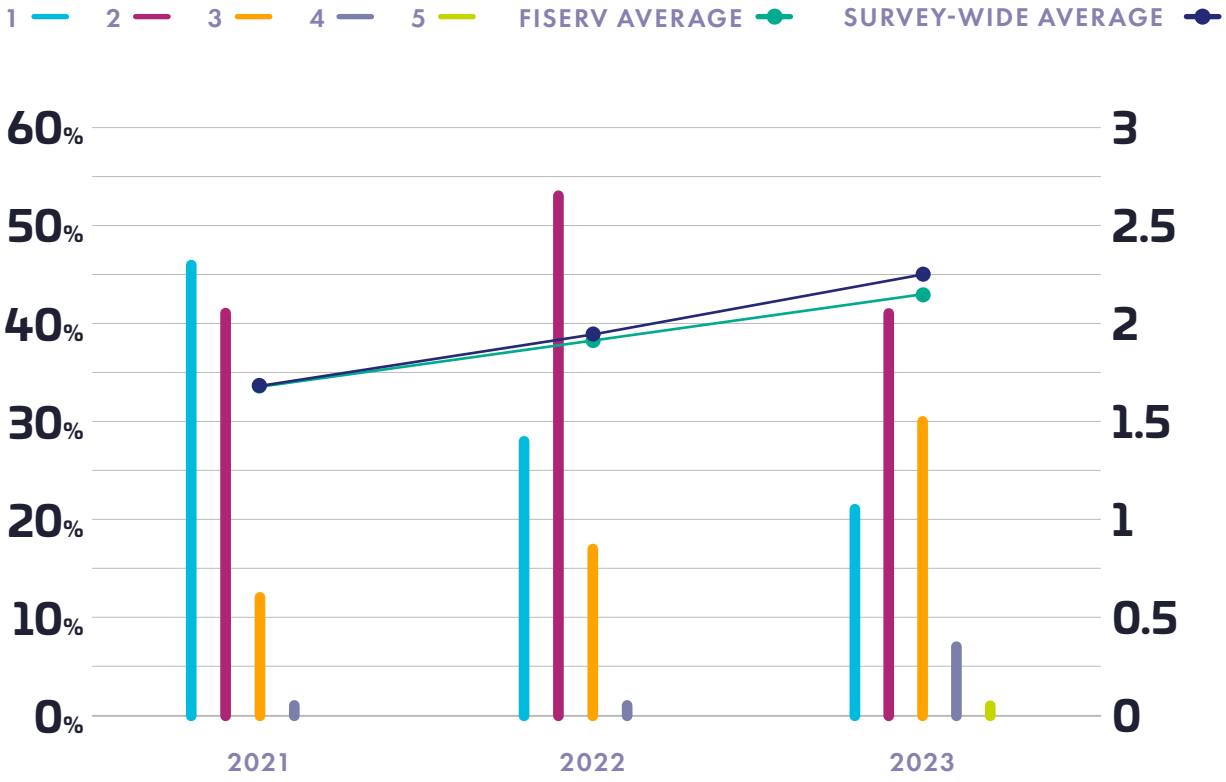
It's a multicloud world

There is increasing multicloud use among FiServ organizations, but it is growing more slowly than in the broad market. The average number of cloud providers increased 12% in the last year (2.16 versus 1.93). FiServ environments are already challenged with securing existing systems that may never move to cloud, while also managing cloud security in an increasing number of locations.

While cloud infrastructure use is lower among FiServ organizations than among the broad survey population, SaaS use is much higher. Broad market respondents report that their enterprises use an average of 97 SaaS applications; in FiServ, that number balloons to 137, or 41% higher. This adds to the number of environments in which data has to be managed and secured.

Number of infrastructure-as-a-service providers in use

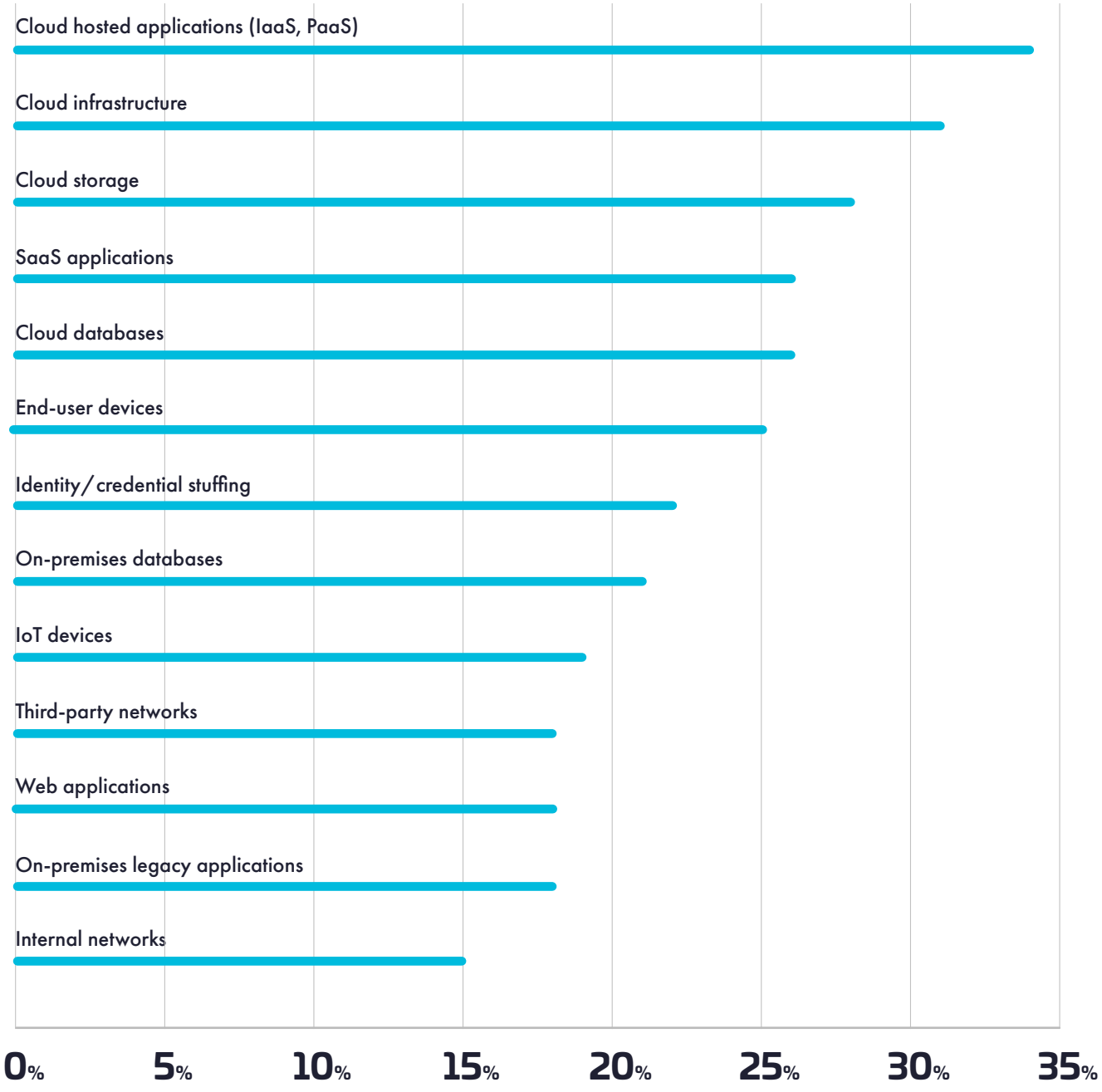
Number of infrastructure-as-a-service providers in use.



Source: S&P Global Market Intelligence's 2021-2023 Data Threat custom survey.

Top cited 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.

The threat landscape for financial services

The threat landscape for FiServ organizations is complex and multifaceted. Cloud-based resources are seen as the leading targets of attackers within the FiServ industry. Cloud-hosted apps are most cited, at 34%, followed by cloud infrastructure at 31%. When looking at cloud infrastructure attacks in detail, third-party attacks lead. This shift in attacker targeting has been reported across industries and reflects an effort to find and exploit the weakest link in an organization's protections. Interestingly, FiServ organizations are more likely to report that credential compromise/credential cracking attacks on their cloud infrastructure are increasing compared to enterprises overall (56% versus 42%). Both of these points reinforce the importance of using more sophisticated authentication technologies with a secured root of trust to manage access, as well as ensuring that foundational data protection capabilities such as encryption are implemented comprehensively and robustly.

Fewer than a third of FiServ respondents (31%) experienced a data breach in their cloud environment in the last year, notably lower than the broad market (40%). The proportion of FiServ respondents who report having ever experienced a cloud breach is slightly lower than the survey-wide result (42% versus 46%).

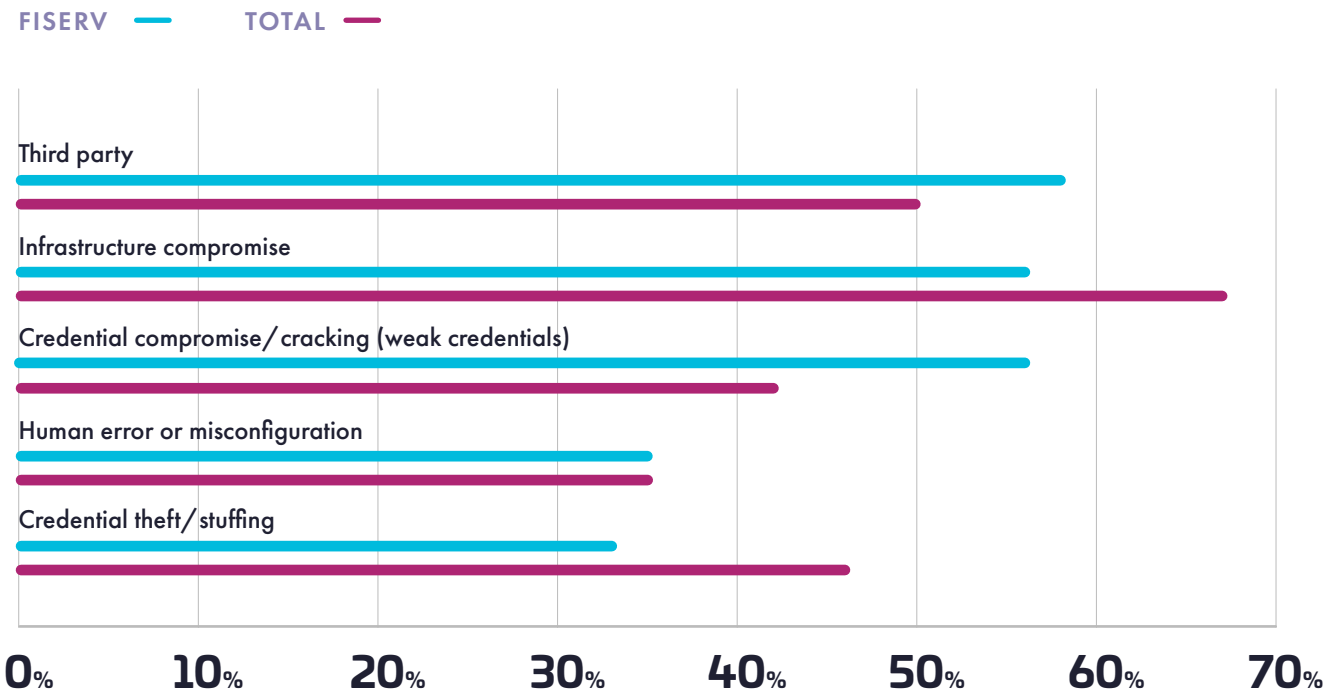
There are widespread concerns about the impact of quantum computing and its potential to break encryption protections. FiServ organizations are a bit more concerned than the total survey population about quantum attacks (98% versus 96%). Perhaps more interesting are the differences in the types of attacks that raise concern. FiServ respondents are more concerned than the broad population about the risks of quantum-based attacks on blockchain (49% versus 43% survey-wide). They are also more concerned about the decryption of network traffic (66% versus 62%).

31%

of FiServ respondents experienced a data breach in their cloud environment in the last year

Types of cloud infrastructure attacks increasing

What type of cloud infrastructure attacks are you seeing increase?



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

Data security concerns

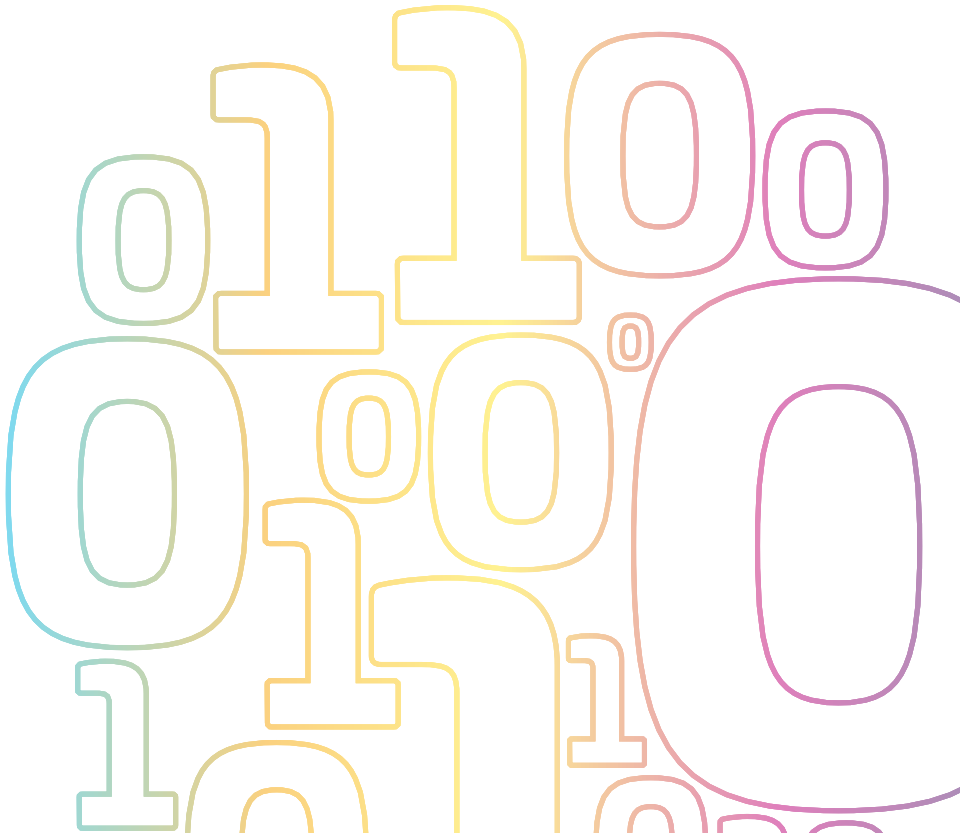
The digitization of many businesses is generating growing volumes of data that must be secured. This is particularly acute in FiServ, where regulatory mandates on both security and resilience are key. The survey shows that an increasing proportion of data resides in cloud-based infrastructure, but the bigger story concerns sensitive data. FiServ organizations report a dramatic increase in the proportion of cloud data that is deemed sensitive. In 2021, 55% of FiServ organizations said that more than 40% of their cloud data was sensitive; this year, that proportion rises to 68%. On average, FiServ respondents say 53% of their cloud data is sensitive. This comes alongside the reporting that only about a third (34%) are able to classify all of their data, a fundamental requirement for effective data protection. It's an improvement from last year (24%), but clearly, this remains a challenge. Just less than half (47%) say that they can classify at least half of their data.

An increasing proportion of sensitive data is being encrypted, but it's still not enough. FiServ respondents on average report that only 46% of sensitive data in cloud is encrypted, which is similar to the broad survey result. But FiServ organizations show greater maturity in the data protections that are in place. More FiServ respondents control all of their own encryption keys compared to the survey-wide sample (21% versus 14%).In multicloud environments, there is more data movement between on-premises, cloud and partner environments. To facilitate secure and efficient movement of data, data management and encryption must work across all environments where data is put to work.

ONLY

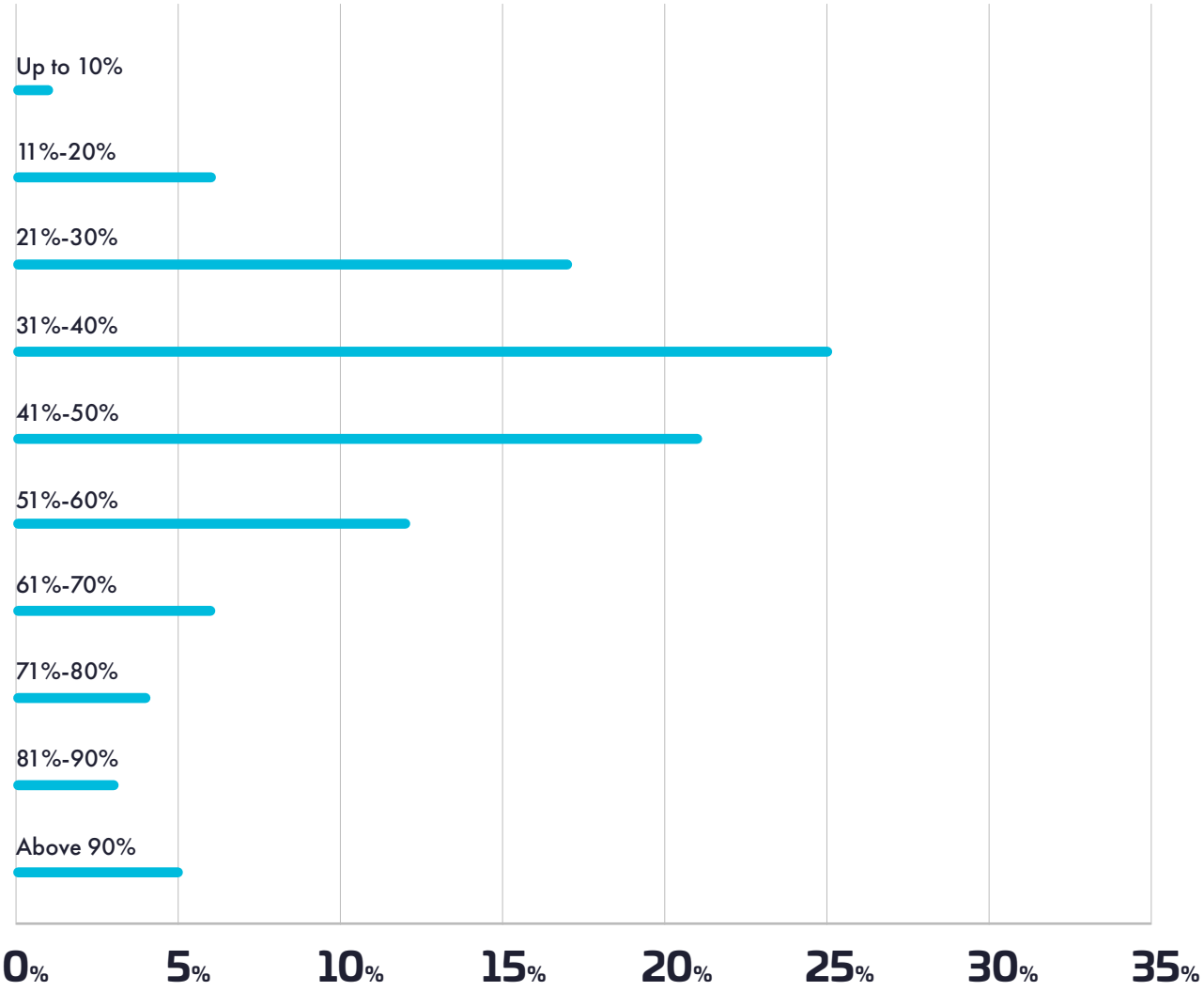
34%

of FiServ organizations are able to classify all of their data



Percentage of sensitive cloud data encrypted

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

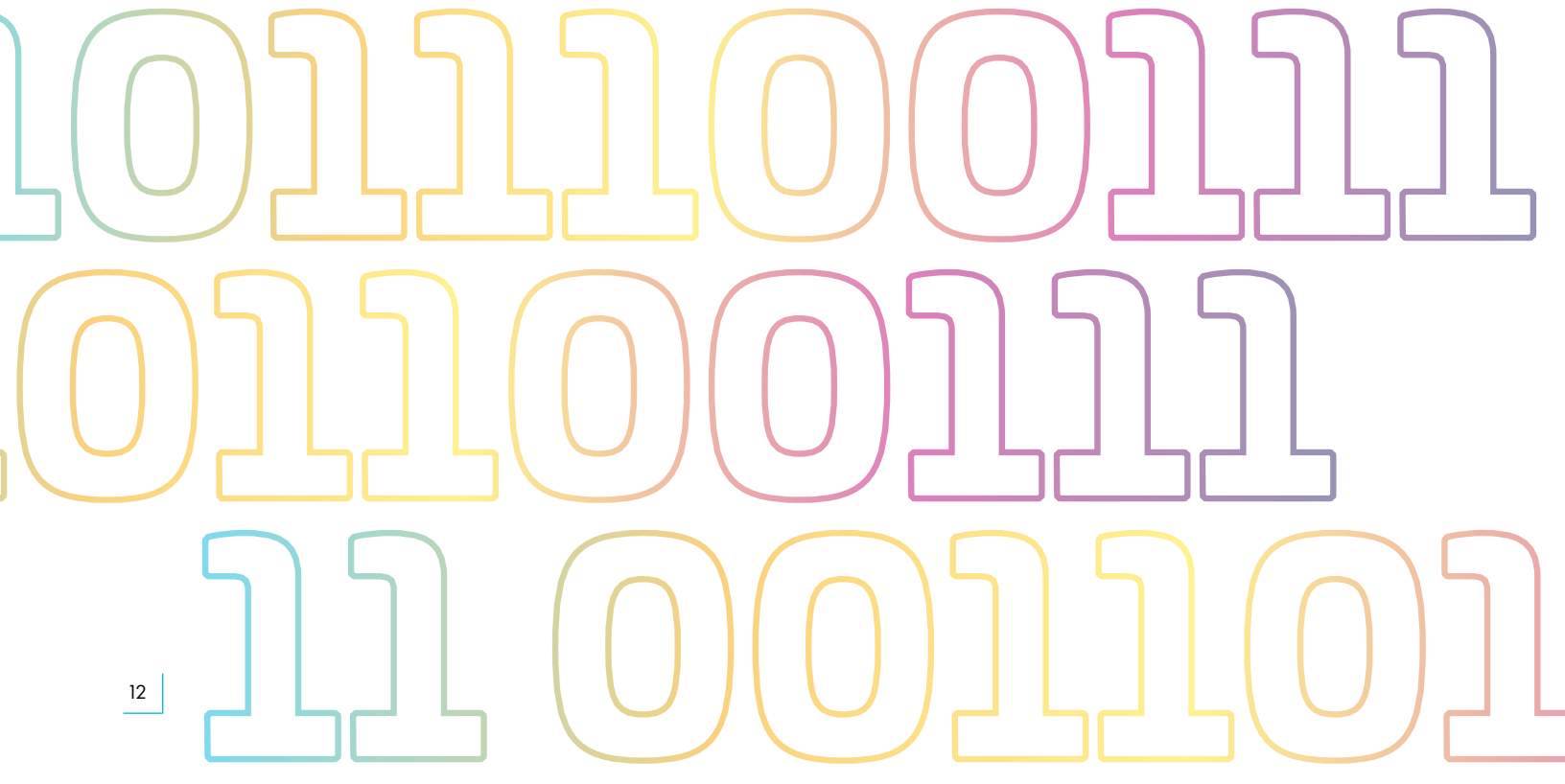


Source: S&P Global Market Intelligence's 2023 Data Threat custom survey.

Impacts of data sovereignty

Digital sovereignty is an emerging strategic initiative and, along with privacy and compliance efforts, it represents opportunities for enterprises to accelerate their digital transformation. Putting better data management controls in place can ensure that stakeholders have access to the data they need, without having to build in controls as part of each new use case. About four-fifths (79%) of FiServ respondents worldwide are "somewhat" or "very" concerned about impacts of digital sovereignty on cloud deployments. That's lower than the survey-wide figure and may indicate that regulatory requirements have already pushed FiServ organizations to implement data controls that could address digital sovereignty requirements.

Almost half of FiServ respondents (44%) consider full data encryption an acceptable measure to achieve various levels of digital sovereignty. This is 5 percentage points higher than the broad survey result. That could indicate greater comfort and confidence in FiServ organizations' data protection capabilities. That said, more than a third (38%) believe that location is important for all of their workloads.



Operational complexity hampers security

One of the largest challenges to overcome in security is operational complexity. Complex operations increase the chance of human error, which FiServ respondents cite as the greatest security threat: 79% select it as a threat, and almost a third of those rank it as their top threat (30%). Human error is also the top reported cause of cloud data breaches and is cited by FiServ organizations to a greater degree than survey-wide (61% versus 55%). Vulnerability exploitation is a distant second at 22%. More than half (55%) of FiServ respondents indicate that it is more complex to manage data in cloud than in on-premises environments.

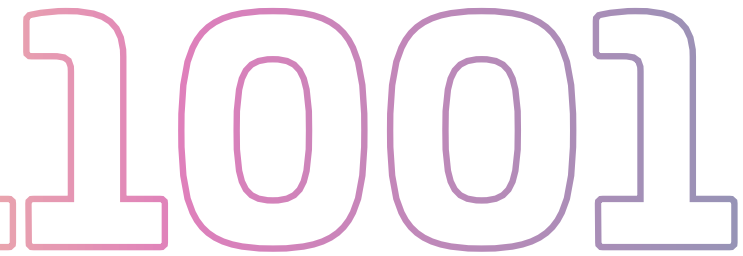
Multicloud infrastructure can increase complexity, particularly when it comes to data encryption. Fewer than a quarter (21%) of FiServ respondents say they control all of their encryption keys in their cloud environments, which, while better than survey-wide, still means the risk of third-party exposure is significant.

Well over half of FiServ respondents say they have five or more key management systems (69%). That's an increase of 4 percentage points over last year, headed in the opposite direction of where it should be and leading to greater operational complexity. If existing key management systems aren't extended to new cloud environments that become part of the production infrastructure, organizations will continue to add silos of key management systems as they grow, compounding complexity and the risk of errors.

ONLY

21%

of FiServ respondents say they control all of their encryption keys in their cloud environments



Pathways to better data security

Identity and access management (IAM) has been identified as a top mitigating control for data breaches. FiServ organizations have reported above-average deployment of strong MFA and a significant increase in adoption, moving from 62% in 2021 to 71% this year. Modern authentication is critical to addressing today's authentication risks.

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. In this year's survey, 41% of FiServ respondents say they have zero-trust controls on cloud networks and 47% have zero-trust in place for cloud infrastructure. That's ahead of the average, which is good news. Interestingly, zero-trust use in internal networks lagged the average (29% versus 36%), an area that could use improvement.

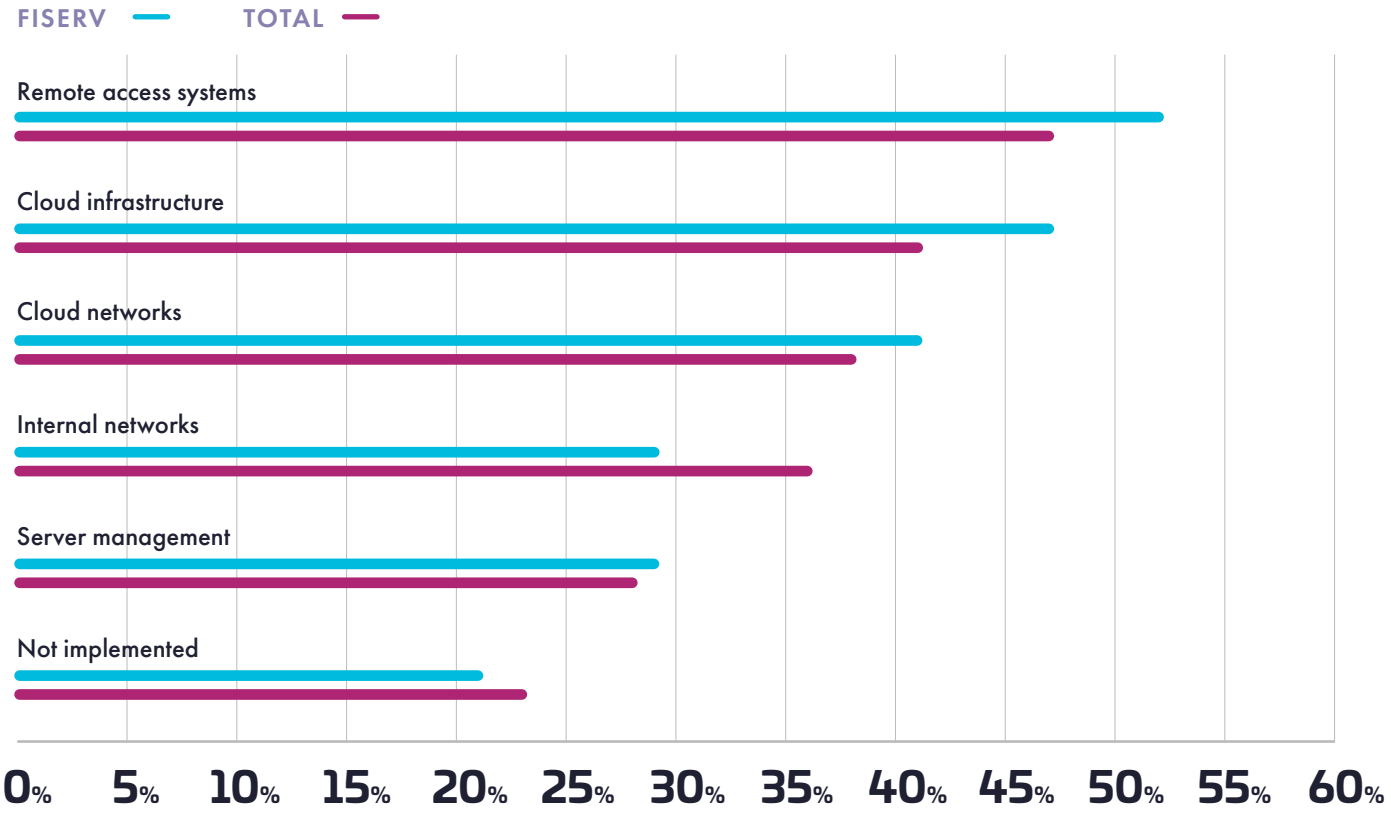
ONLY

41%

of FiServ respondents say they have zero-trust controls on cloud networks

Implementation of zero trust by financial services respondents

How does your organization use zero-trust practices?



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

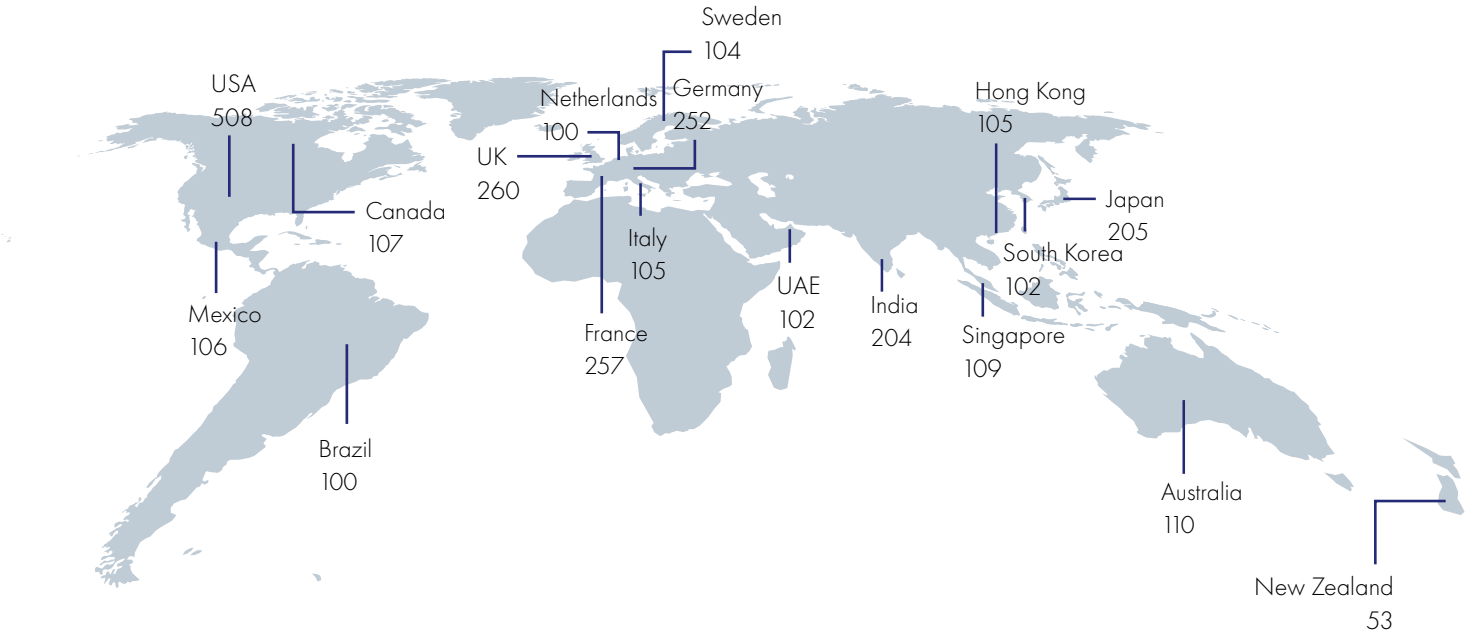
Moving ahead

FiServ organizations face a unique set of risks and additional complexity in managing data security. Digital transformation and rising regulatory pressures have led to increases in both the volume of data and the imperatives to secure it. At the same time, expanding data ecosystems and multicloud infrastructure are creating the need to move more data to more locations.

To address these challenges and overcome issues with human error and misconfiguration, data protection needs to become simpler to manage. Delivering effective and efficient security requires increased automation and consolidated management to cope with expanding infrastructure and scale. Organizations that put in the effort receive dual benefits: improved security posture and increased ability to meet compliance requirements. FiServ organizations have been making progress and, in some cases, are ahead of the average enterprise, but there is still much more to do.

About this study

This research is based on a global survey of 2,889 respondents, of which 140 were from financial services 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 regarding the level of knowledge about 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/financial-services-data-threat-report