THALES
Building a future we can all trust

GLOBAL EDITION

2023 DATA THREAT REPORT

Perspectives and Pathways to Digital Sovereignty and Transformation

#2023DataThreatReport
cpl.thalesgroup.com

Introduction

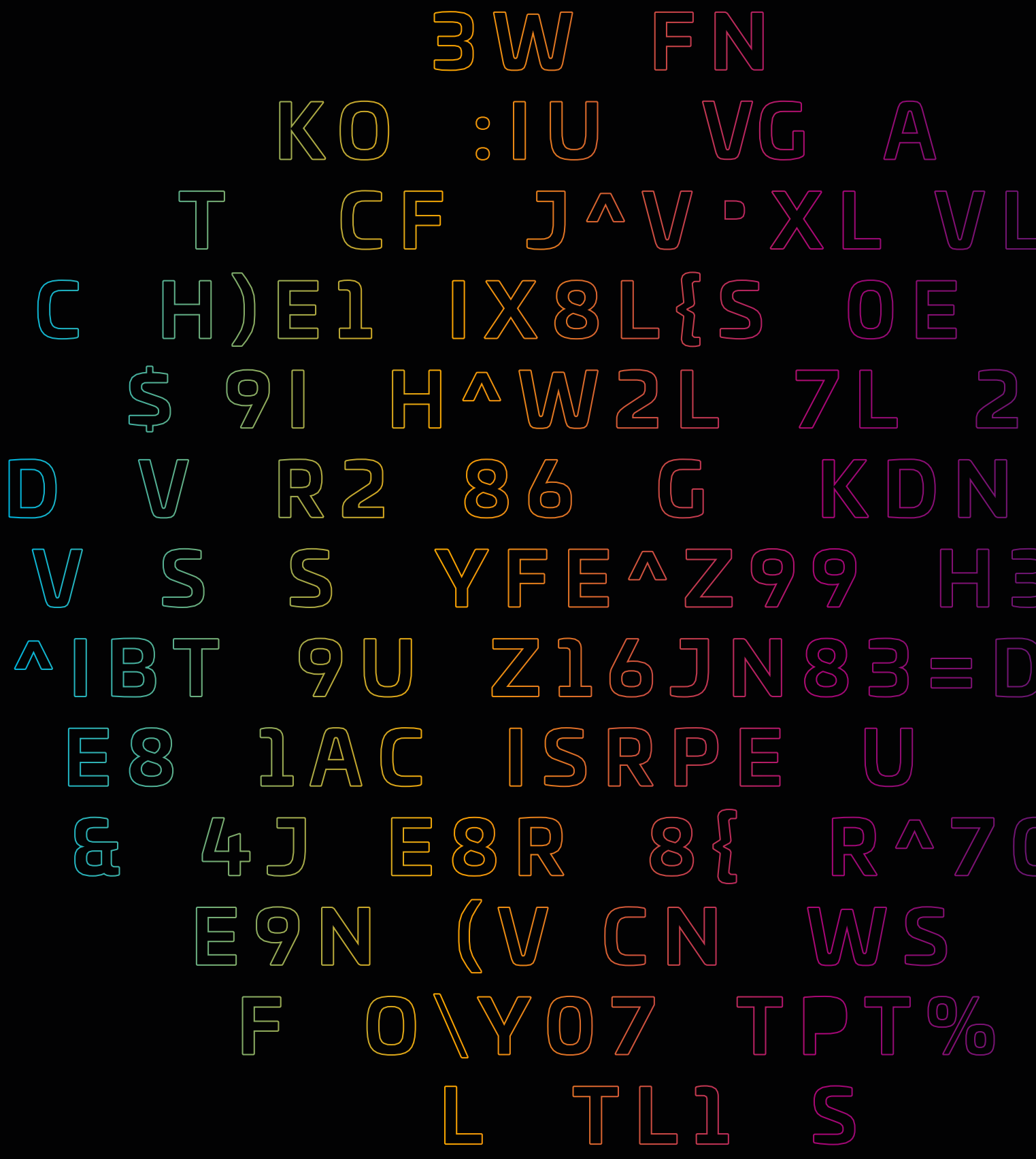
Despite the economic and geopolitical tensions that arose in 2022, enterprises continued to invest in their operations and their digital transformation. Organizations balanced security and privacy risks with opportunities opened by new technologies and business models. The 2023 Thales Global Data Threat Report, conducted with nearly 3,000 respondents across 18 countries, in roles ranging from senior executive leaders to individual practitioners, illustrates how influencers and decision-makers manage this balance; considers their attitudes, perceptions, realities and expectations for the years ahead; looks at the influencers and decision-makers driving enterprise security policies and practices; and highlights changes over time.

S&P Global
Market Intelligence

Source: 2023 Data Threat Report custom survey from S&P Global Market Intelligence, commissioned by Thales.

Sponsored by

EXCLUSIVE NETWORKS


3W FN
KO :IU VG A
T CF J^V·XL VL
C H)E1 IX8L{S OE
$ 9I H^W2L 7L 2
D V R2 86 G KDN
V S S YFE^Z99 HE
^IBT 9U Z16JN83=D
E8 1AC ISRPE U
& 4J E8R 8{ R^70
E9N (V CN WS
F O\Y07 TPT%
L TL1 S

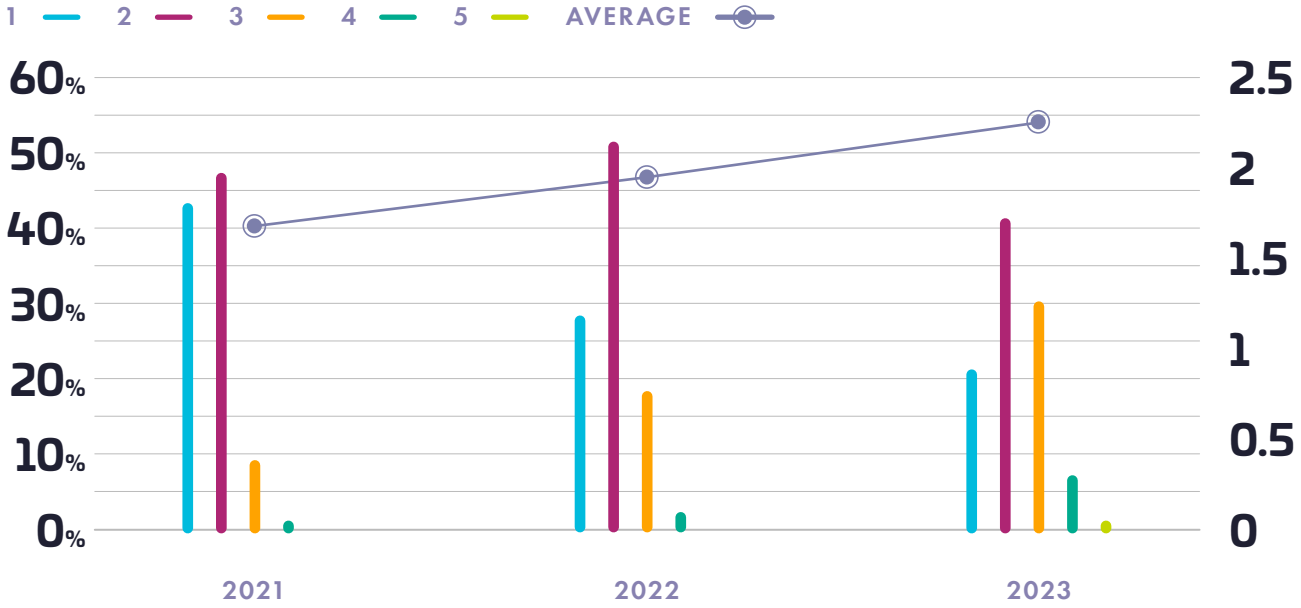
Contents

Digital transformation continues to accelerate

Digital transformation continues to accelerate in enterprises despite inflation, market volatility and geopolitical instability. Many private enterprises continue to thrive, with the S&P 500 still recording historically high levels of profitability in 2022. This profitability drives enterprises to invest in further automating and transforming their operations with new technologies and greater cloud adoption. One of the first observations is the greater diversity of cloud services, technology and personnel. Even organizations that employ more conservative cloud deployment strategies such as "lift and shift" report strong multicloud adoption. Respondents representing companies with lift-and-shift strategies report using at least two cloud providers for production workloads across AWS, Google, Azure, Alibaba, Oracle and IBM.

Multicloud is the rule, not the exception

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

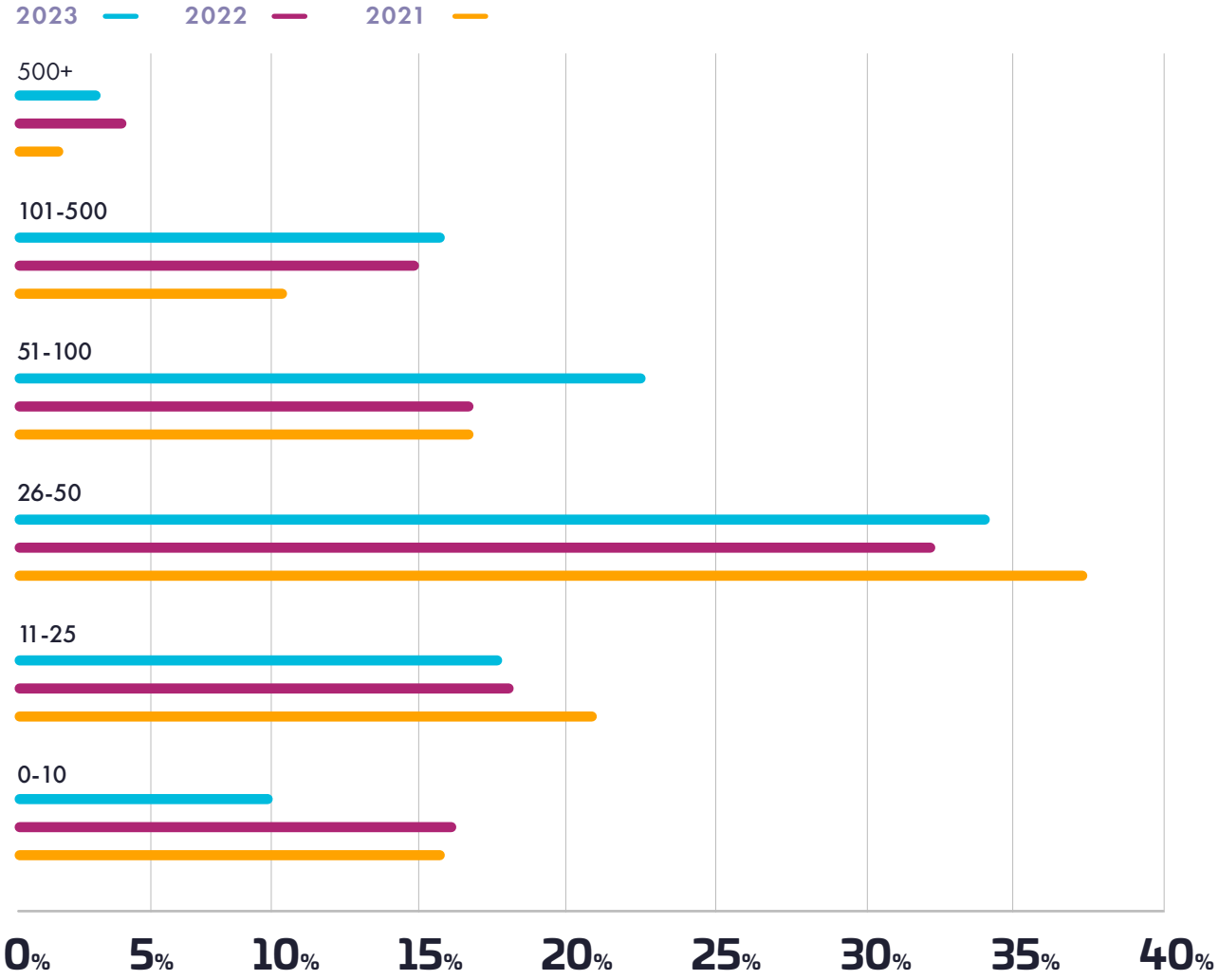


Source: S&P Global Market Intelligence's 2021-2023 Data Threat custom surveys

The diversity of enterprise SaaS adoption has also been increasing. In 2021, 16% of respondents reported that their enterprise was using 51-100 SaaS applications; in 2023, the percentage using 51-100 SaaS applications has risen to 22%.

SaaS diversity is trending higher

How many Software as a Service (SaaS) applications does your organization use?



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

Can data security adapt?

While many digital transformation initiatives have resulted in new sources of revenue and greater profit for enterprises, security collaboration has lagged. Digital transformation initiatives require changes in approach with greater security collaboration built in. As enterprises adopt new technologies for transformation, they realize the risks with renewed concern. According to survey respondents in ranked-choice voting, the greatest risks in cloud operations are infrastructure compromise (67%) and third-party risk (50%). Complexity remains a top barrier to securing multicloud environments for the third year in a row. The number of respondents who "agree" or "strongly agree" that it's more complex to maintain privacy and data protection regulations in the cloud has grown from 46% to 50% to 55% in 2021, 2022 and 2023, respectively.

In the shadow of new geopolitical realities, digital sovereignty and privacy have emerged as top concerns that data management technologies must address. In a new finding from this year's report, 83% of respondents are "very" or "somewhat" concerned about digital sovereignty. Three-fourths of respondents have security concerns about new technologies such as 5G (77%). Risks from existing threats also continue with 48% of respondents saying ransomware attacks are still increasing.

The 2023 Thales Data Threat Report contrasts expectations and attitudes with results and realities to better illustrate how enterprises can make plans and secure controls to continue their digital transformation journey. This report studies how enterprises respond to and plan their data security strategies and practices in the light of the changing regulatory, technology and threat landscapes and offers insights into possible directions.

Key findings

We're only human:

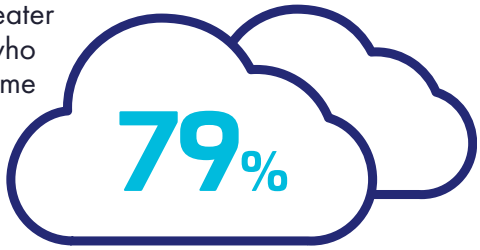
The #1 root cause of cloud data breaches is human error

65%

Strong MFA adoption increased to 65% and 28% of respondents identified IAM as the top security technology most effective in protecting sensitive data from cyberattacks.

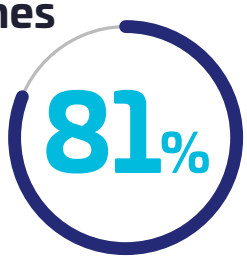
Multicloud is a reality, regardless of cloud maturity.

Four-fifths (79%) of enterprises have production workloads in more than one public cloud, significantly greater than the 57% who reported the same in 2021.



While internal security attitudes are improving, security outcomes continue to lag.

81% of respondents are still confident to trust their personal data to their systems.



Yet 37% said they had a breach in the last 12 months.

Digital sovereignty is an emerging strategic initiative.

83% of respondents were very or somewhat concerned that data sovereignty and/or privacy regulations will affect their organization's cloud deployment plans.

96% of respondents consider designating or changing the location and jurisdiction or full data encryption are acceptable measures to achieve various levels of digital sovereignty.

Cloud risk awareness is catching up with cloud adoption.

77%

had security concerns around 5G. Of those with concerns, 75% said protecting the identities of people and devices connecting to 5G networks was the top concern.

38%

SaaS apps and cloud-based storage was identified as the top target for cyber attacks

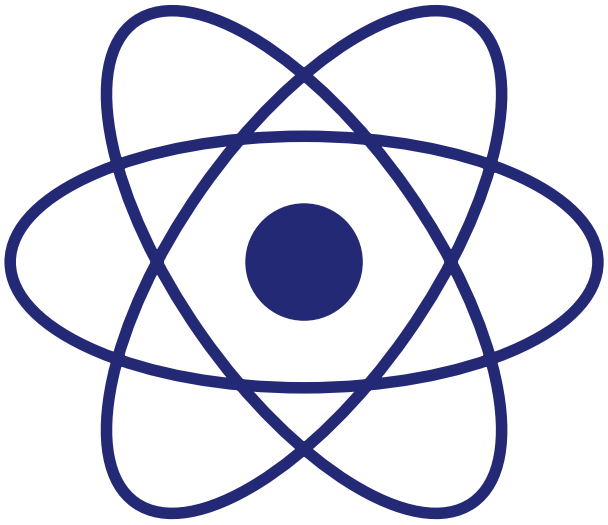
Growing complexity of Hybrid IT challenges data security architectures

62%

55%

62% of enterprises have at least 5 enterprise key management systems adding to the complexity.

55% agree that it is more complex to manage privacy and data protection regulations in a cloud environment than on-premises networks.



Post quantum cryptography moves further from the academic to the real world.

Enterprises should begin today to inventory and simplify their encryption deployments.

ONLY 49% of organizations have a formal ransomware response plan, compared to 48% in 2022 when we first asked.

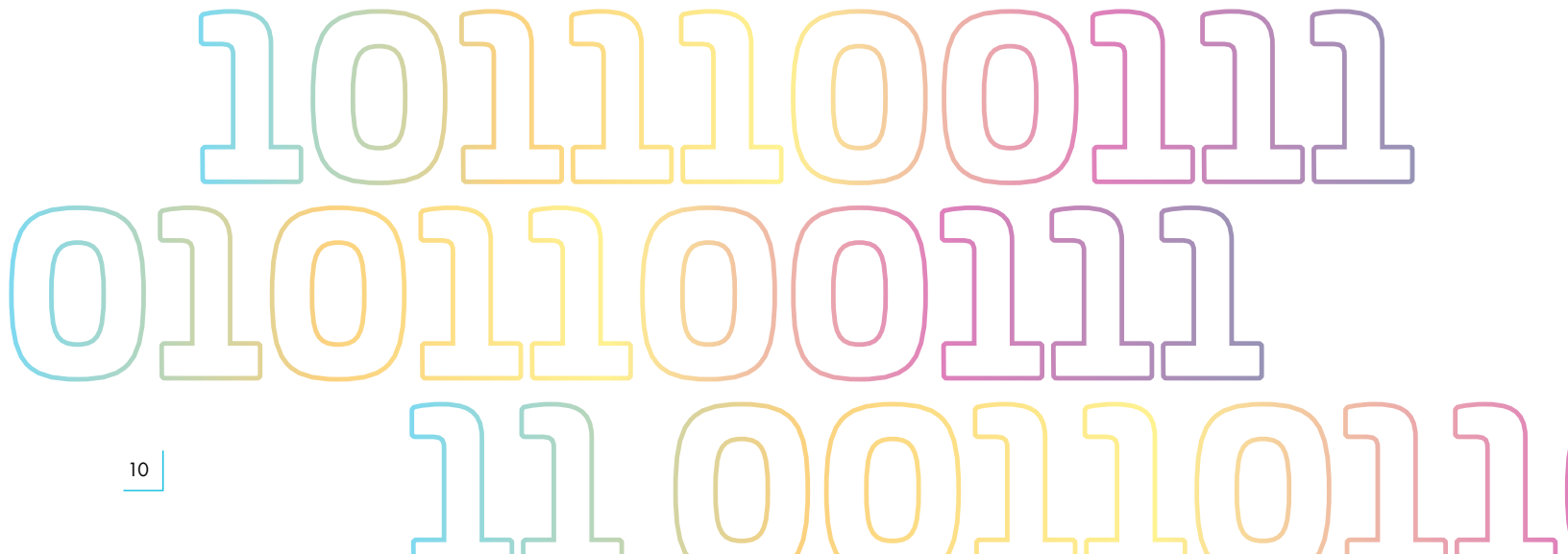
The threat landscape ahead

Respondents continue to see a serious threat landscape ahead. Nearly half (47%) of respondents say that attacks are increasing in volume or severity, similar to reported numbers in 2021 and 2022. Of those respondents seeing an increase in attacks/threats, 59% report increases in malware, 48% report increases in ransomware and 43% have seen an increase in phishing attacks. The primary types of threats increasing and the percentage of respondents identifying them have remained consistent for the last three years. Of those seeing threat increases in 2022, malware, ransomware and phishing were at 56%, 53% and 40%, respectively. In 2021, malware, ransomware and phishing were at 54%, 48% and 40%, respectively.

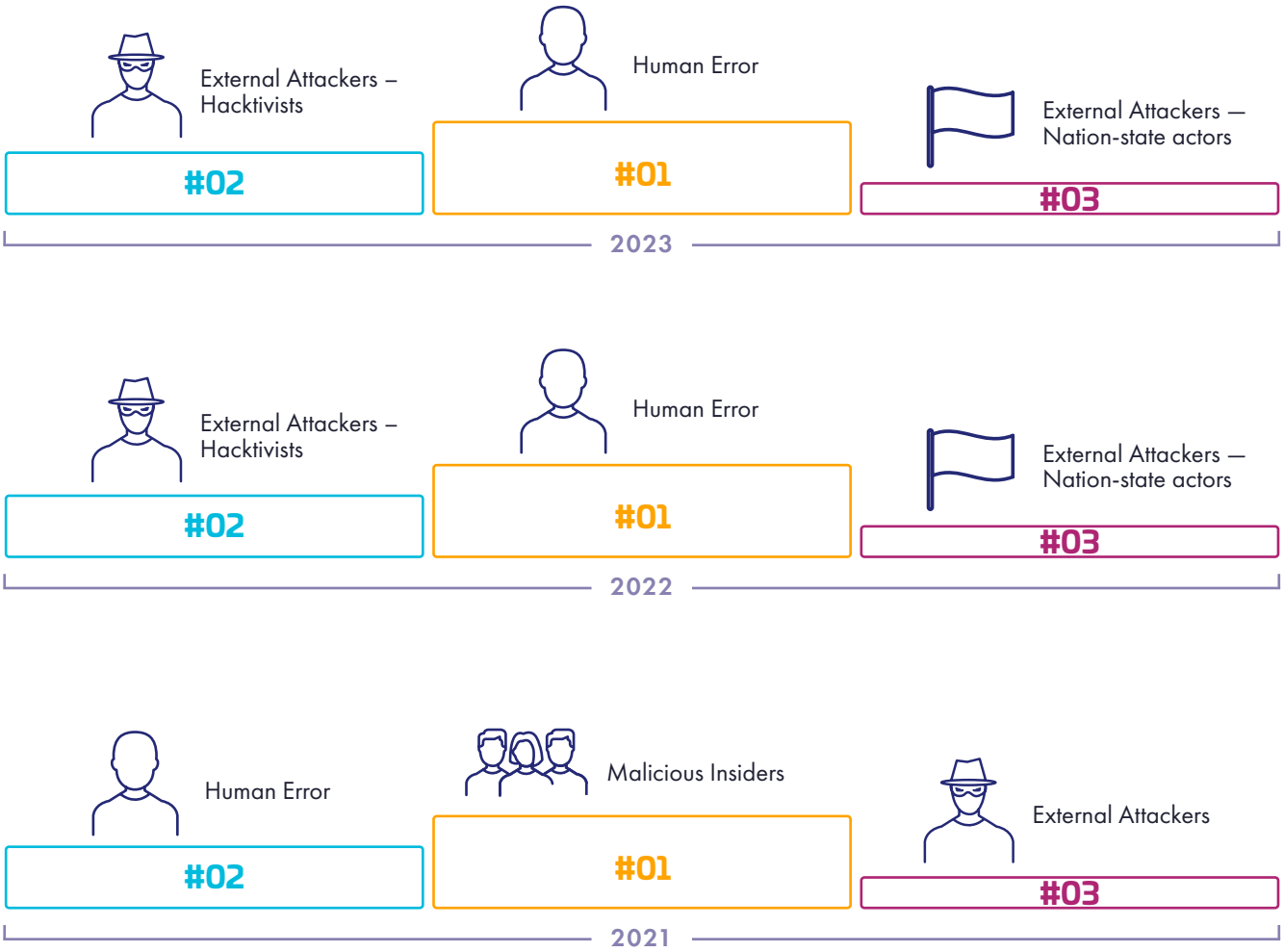
However, the reported threat sources have changed. In absolute terms with ranked choice voting, this year's respondents prioritize human error, external hacktivists and nation-state actors, chosen by 77%, 76% and 72%, respectively. In previous years, malicious insiders were more of a concern.

59%

of respondents say they have seen an increase in the volume or severity of Malware attacks.



Which types of threats are you most concerned about?



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

Enterprise responses to threats continue to lag. For starters, only 65% of enterprises say they are confident that they know their data's location. While enterprises cannot control external threats, they can lessen the impact and their vulnerability by better identifying their assets and adapting their transformation journey to incorporate security.

64%

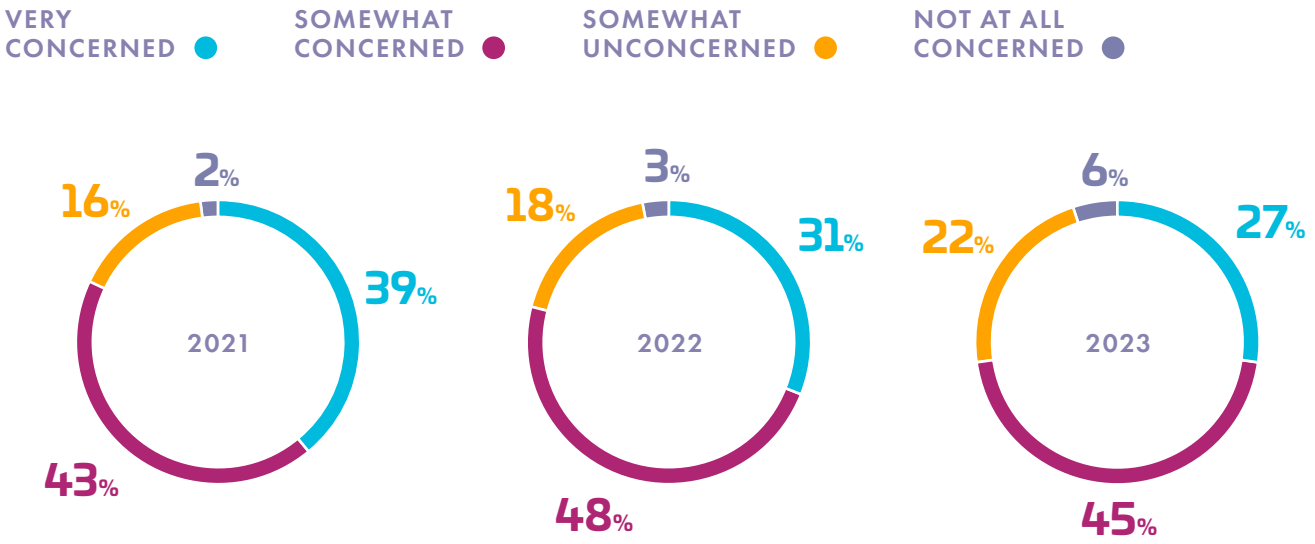
Only 64% of European enterprises with annual revenue of more than $1 billion say they are "very confident" or have "complete knowledge" of their data's location.

Internal attitudes

With human error identified as a leading cause of security concerns, and with poor security outcomes continuing to challenge enterprises, the 2023 Data Threat Report looks at internal attitudes and examines how enterprises are responding internally. Like the 2022 report, 81% of respondents say they would trust their enterprise's systems to secure and manage their personal data. This level of confidence remains consistent among roles ranging from security practitioners to senior finance, legal and regulatory leaders. Concerns about risks from remote work remain high, but these are softening. Just over a quarter (27%) of respondents report that they are "very concerned" about remote work risks, a 4-percentage-point drop from 2022 and 12 percentage points lower than in 2021.

Remote Work

How concerned are you about the security risks/threats of employees working remotely?



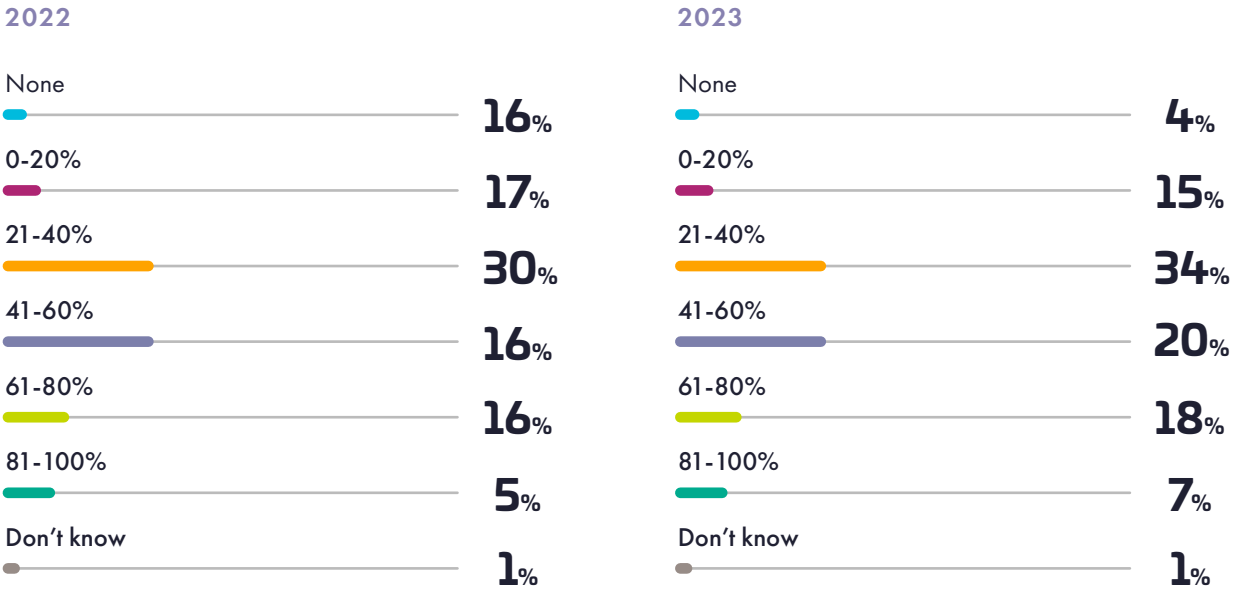
Source: S&P Global Market Intelligence's 2021-2023 Data Threat custom surveys

57% **are confident in their organization's access security solutions to enable secure and easy remote work.**

Respondents indicate an increase in positive user behavior; adoption rates of MFA/modern authentication serve as a barometer of user security culture and awareness. Authentication is a distinct user experience that affirms something known (passwords) and possessed (tokens). Authentication is arguably the most distinctive, frequent security experience for all users. Current or planned MFA adoption was flat at 55% for 2021 and 2022; in 2023, it has jumped to 65%. Moreover, the use of MFA specifically for SaaS apps is trending upward.

Percentage of employees using strong authentication for SaaS/ cloud apps

What percentage of employees use strong authentication for SaaS/Cloud applications?

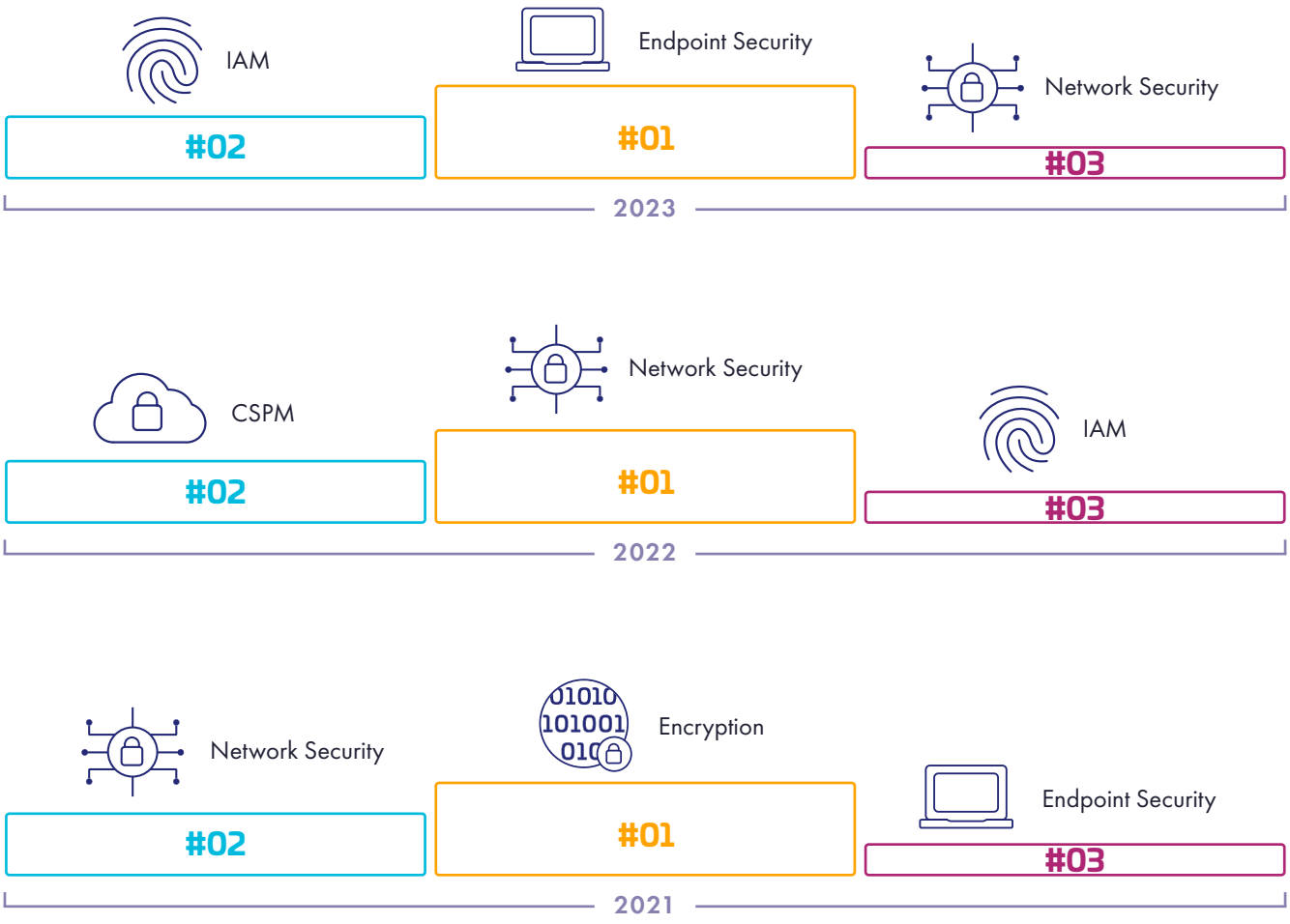


Source: S&P Global Market Intelligence's 2022-2023 Data Threat custom surveys

While increased MFA adoption rates reflect better end-user awareness and security culture to mitigate leading threats such as human error, there remains some disconnect in what controls can protect sensitive data going forward. While respondents indicate that IAM is one of the most effective technologies to protect sensitive data, ranked-choice voting also reveals a variety of other controls.

Controls considered most effective for protecting sensitive data (ranked choice)

Which security technologies are most effective in protecting sensitive data from cyberattacks?



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

Anticipating new technologies

The threat landscape and prevailing attitudes face continued changes in new technologies that enterprises are adopting or anticipate adopting. New technologies such as 5G, edge computing and IoT are redefining how compute infrastructure is provisioned, utilized and secured. A new finding in this year's report is that 77% of respondents report security concerns about 5G. Of those with 5G security concerns, 75% say protecting the identities of people and things connected to 5G networks is their greatest concern, and 66% say they are most concerned about the security of data moving across 5G networks.

Within existing cloud deployments, respondents also report a greater diversity of cloud infrastructure. Eighty percent of respondents are using one or more cloud service providers for a production workload.

Multicloud remains the rule for enterprises across all geographies, cloud strategies, verticals and enterprise sizes. Cloud adoption across cloud service providers continues to grow, reflecting multicloud diversity.

77%

of respondents had security concerns around 5G.

75%

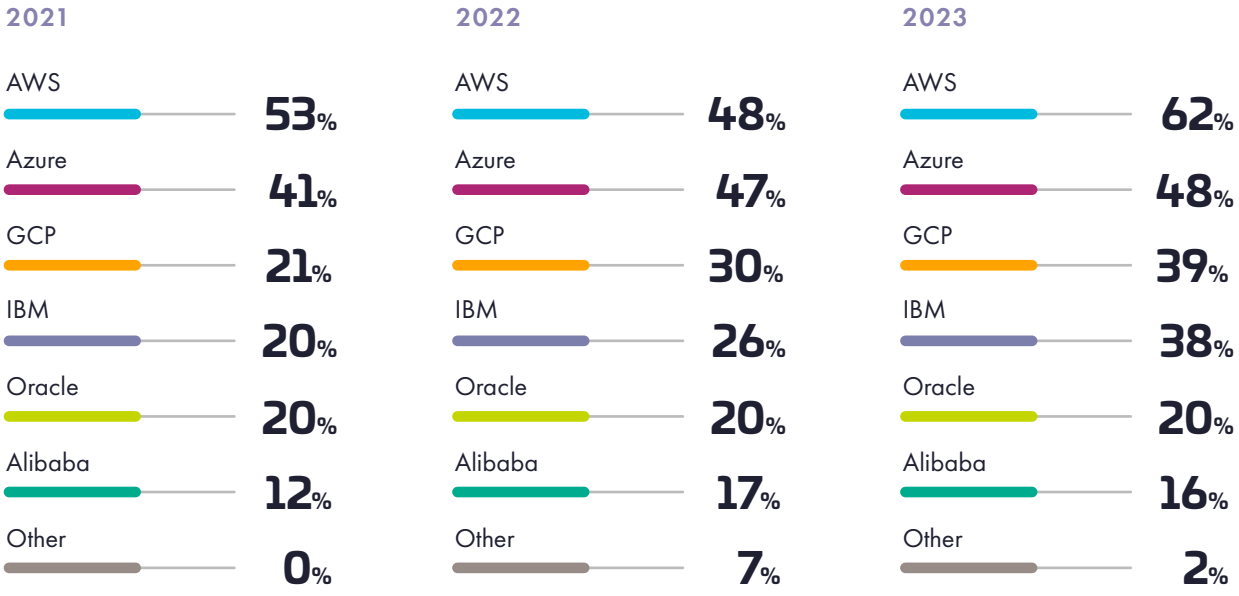
of those with concerns, protecting the identities of people and devices connected to 5G networks was the top concern, with 75% saying so.

2.26

On average, respondents are using 2.26 cloud service providers.

Cloud service providers in use

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 2021-2023 Data Threat custom surveys

As noted above, a large majority (80%) of respondents currently use cloud for production environments, while the remaining 20% are in pilot or near-term (less than 12 months) adoption phases. Cloud prevalence, and its capability for enterprises to employ new technologies with less opportunity cost, will continue to drive enterprise adoption and will only increase the pace of technological change.

External expectations — new risks

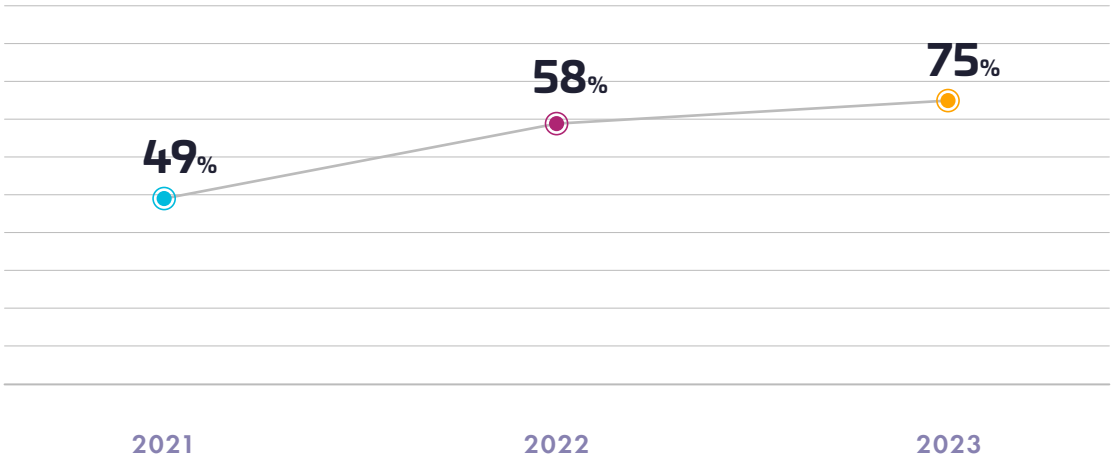
While respondents are eager to adopt new technologies, they are also aware of the inherent risks. From 2021 through 2023, the percentage of respondents who "agree" or "strongly agree" that it is more complex to maintain privacy and data protection regulations in the cloud has steadily grown from 46% to 55%.

Despite the complexity, more companies are putting more of their sensitive data in the cloud, and they have a higher proportion of sensitive data to overall data. This means a concurrent increase in data risks over time. In 2022, 52% of respondents said that more than 40% of all their sensitive data was stored in the cloud. This percentage increased in 2023, with 64% of respondents saying that more than 40% of their sensitive data is stored in the cloud. The concentration of sensitive data in the cloud has also increased (thus increasing data risk). In 2021, 49% of respondents said that more than 40% of their cloud data was sensitive. That level has increased significantly: 58% of 2022 respondents and 75% of 2023 respondents indicated that more than 40% of their cloud data is sensitive.

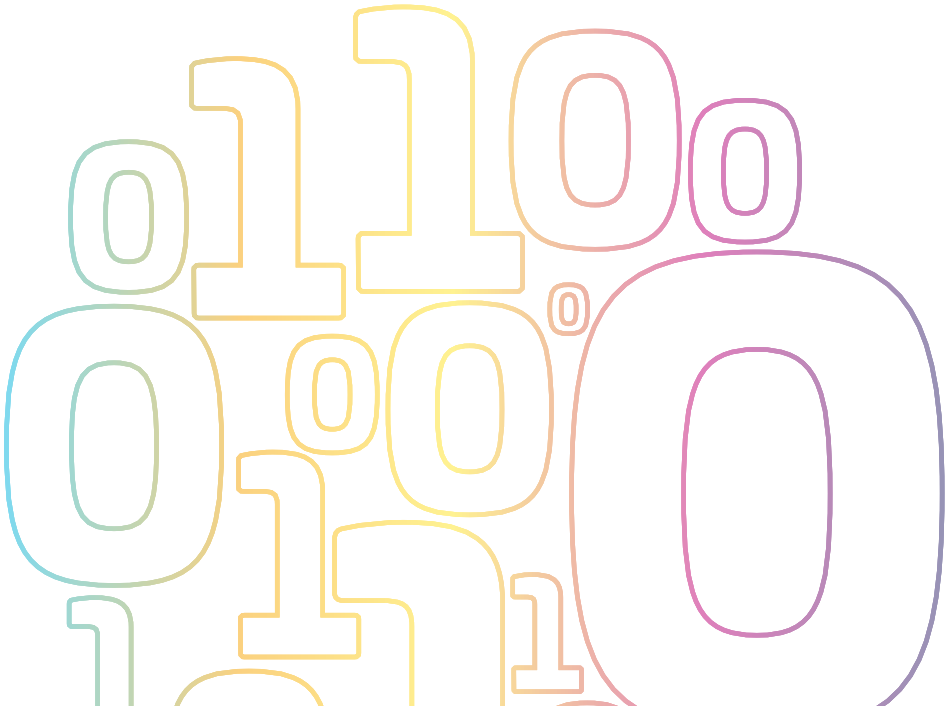
Given the shifting of sensitive data toward the cloud and the greater concentration of sensitive data in the cloud, it is not surprising that respondents identify their cloud assets as the biggest targets for cyberattacks. In ranked-choice selections, 28% said that SaaS apps and cloud-based storage, 26% said cloud-hosted applications or cloud databases in IaaS/PaaS, and 25% said cloud infrastructure were the top attack targets. Regarding cloud infrastructure attacks, respondents are seeing increases in infrastructure compromise and third-party risk. In general, enterprises are tempering their organization's eagerness to transform using new technologies with greater risk awareness.

Sensitive Cloud Data Has Risen

The concentration of sensitive cloud data (the percentage of respondents who say more than 40% of cloud data is sensitive) has dramatically risen.



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



External events and the accompanying risks

So far, the 2023 Data Threat Report has revealed how enterprises perceive the external threat landscape, explored how they have changed their internal security attitudes and examined how enthusiastically they are adopting new technologies to competitively transform while balancing that enthusiasm with a greater awareness of risks from new technologies. Yet, organizations must also consider broader external events beyond their control. Just as the COVID-19 pandemic had a large effect on respondents to the 2021 and 2022 Data Threat Reports, notable external events affected 2023 respondents as well:

- Sovereign clouds gained traction as several countries enforced digital sovereignty and data localization.
- US presidential mandates on zero trust took effect in Executive Order 14028.
- The National Institute of Standards and Technology approved four algorithms for PQC key exchange and digital signatures. Ratified legislation mandating post-quantum cryptography safety passed in December 2022.
- In response to the "Schrems II" case, US President Biden's Executive Order 14086 looks to overcome objections and build a path toward restoring the EU-US privacy shield.
- Several states in the US passed or amended privacy regulations. Regulations from the California Consumer Privacy Act were extended further with the California Privacy Rights Act, which takes effect in 2023.
- European industry looked to become more self-sufficient, not just in its sourcing of energy, but extending to the desire for digital self-sufficiency. Echoing the sentiment of self-sufficiency, the US passed the Chips and Science Act in August 2022.

With significant developments in external events, it remains important for enterprises to continue to consider data security a board-level initiative and to prioritize in the context of changing and growing regulations. In certain segments such as finance, regulations are growing at unprecedented rates. Security, technology, product and line-of-business leaders should work with their legal and governance teams to prioritize data security initiatives, with the understanding that regulatory priorities are growing.

Security disciplines will continue to be preventative or corrective, yet increasingly, their efficacy will be determined by how readily enterprises can apply them. Security strategy must respond to these external events and put changing regulations into context for enterprises to progress. Digital sovereignty is the most significant external challenge for enterprises to respond to; it requires immediate attention and has long-term strategic implications.

Growing Regulations. According to the S&P Global Market Intelligence Cappitech Global Regulatory Reporting Survey 2022, global regulatory reporting is an increasingly important consideration as regulators add new or extend existing regulations. 99% of respondents have obligations in at least two regimes and a solid 13% are reporting in more than ten.

99% of respondents have obligations in at least two regimes and a solid 13% are reporting in more than ten."

Anticipating digital sovereignty

More than half (55%) of respondents "agree" or "strongly agree" that data protection and compliance in the cloud is more difficult than in on-premises environments. The emergence of digital sovereignty adds further challenges to cloud data protection and compliance.

Digital sovereignty is the ability for enterprises to have more control and freedom with the data, hardware and software used in their offerings and services. Digital sovereignty enables enterprises to have better localized enforcement of privacy laws to maintain safe data stewardship of sensitive and publicly identifiable information to adhere to different privacy, data security and resilience regulations worldwide. Digital sovereignty represents a significant opportunity for enterprises to optimize their systems and architectures while better serving stakeholders and citizens.

Regarding digital sovereignty specifically, 83% of respondents worldwide say they are "somewhat" or "very" concerned. Nearly all (96%) respondents say that either designating the location/jurisdiction of data or implementing full data encryption are acceptable methods to achieve varying requirements of cloud/digital sovereignty.

Digital sovereignty remains both a short- and long-term challenge for enterprises. In the short term, current privacy legislation demands immediate action for enterprises. For the longer term, digital sovereignty requires enterprises to consider the sovereignty of data, operations and software.

83%

of respondents were very or somewhat concerned that data sovereignty and/or privacy regulations will affect their organization's cloud deployment plans.

Data sovereignty means enterprises must maintain control over data. Data security enforced with encryption and access controls restricts data from foreign and unauthorized use. Encryption keys can even be managed separately from the cloud provider itself. Operational sovereignty provides enterprises control over public cloud provider operations, such as limiting access for cloud provider support personnel. Software sovereignty means running workloads without dependence on a cloud provider's software. This freedom helps enterprises avoid lock-in or dependency on proprietary tools, which is particularly relevant given the number of multicloud organizations.

With these challenges in digital sovereignty affecting internal attitudes, external realities and technology expectations, enterprises may feel like data security is too daunting. Yet a way forward for respondents may be to continue iterating successfully on current data security initiatives. For example, only about 20% of respondents report that more than 60% of their cloud data is encrypted. The different data owners and stewards must collaborate more closely in the lifecycle through which data is created, accessed, processed and stored.

20%

Only about 20% of respondents report that more than 60% of their cloud data is encrypted.

Gaps between intention and implementation must be closed. While relatively few enterprises have encrypted most of their cloud data, the vast majority intend to do so, and they possess knowledge of encryption schemes. For example, regarding how they encrypt IaaS/PaaS data, 55% of respondents say most or all of their applications use cloud provider encryption products, 36% bring their own encryption tools for most of their workloads, and the remaining 9% use a blend of tools depending on workload.

Similarly, enterprises should be prepared to be flexible with a variety of encryption schemes to serve different operational and data sovereignty requirements. More than half (59%) of respondent enterprises have delegated all or most of their encryption key control to their cloud service provider. This approach makes sovereignty more difficult to achieve because encryption key control cannot be repurposed independently of the cloud. As more enterprises pursue multicloud strategies and are required to maintain digital sovereignty and control, encryption key control and operation should be independent of any single cloud provider. Of the enterprises that control their own encryption keys, 54% report that they manage them through cloud consoles, and of those, 29% use a hold-your-own-key (HYOK) and 45% use a bring-your-own-key (BYOK) scenario.

59%

of respondent enterprises have delegated all or most of their encryption key control to their cloud service provider.

Digital sovereignty represents both a short-term and long-term opportunity for enterprises. While changing data regulations require more immediate responses, the long-term data, operational and software independence from any single cloud provider gives the enterprise the foundation to embrace new cloud technologies to strategically grow.

Ransomware – responses, results and realities

For data security practitioners as well as line-of-business, regulatory and technology teams, perhaps no collaboration is more urgent than when mission-critical operations are unavailable. In general, the speed and severity of ransomware attacks bring security program effectiveness and its organizational impacts into sharp, immediate focus. Starting in the 2022 Data Threat Report and again this year, respondents shared their ransomware responses, results and realities.

The occurrence of ransomware increased slightly from the 2022 report; 22% of respondents have experienced a ransomware attack, compared to 21% in 2022. Fortunately, however, the severity of attacks declined. Just over a third (35%) of affected respondents say their ransomware incident had a significant impact or external operations exposure, compared with 44% saying the same in 2022. Still, 67% of affected respondents say they experienced some data loss from the attack.

Organizational responses to ransomware remain inconsistent. Only 49% of enterprises use or have created a formal ransomware plan (unchanged from the 2022 report). One-fifth (21%) of 2023 respondents say they paid or would pay ransoms, despite legal questions about doing so. Respondents say the greatest impact of a ransomware attack was or would be financial-based, such as fines and penalties, rather than "softer costs," such as loss of productivity. 2023 respondents indicate that the cost of recovery and financial losses are the top two greatest impacts of ransomware attacks. The absence of formal plans to dictate engagement with internal/external personnel, law enforcement intervention or even ransom payment itself is a risk, with potentially severe downsides.

67%

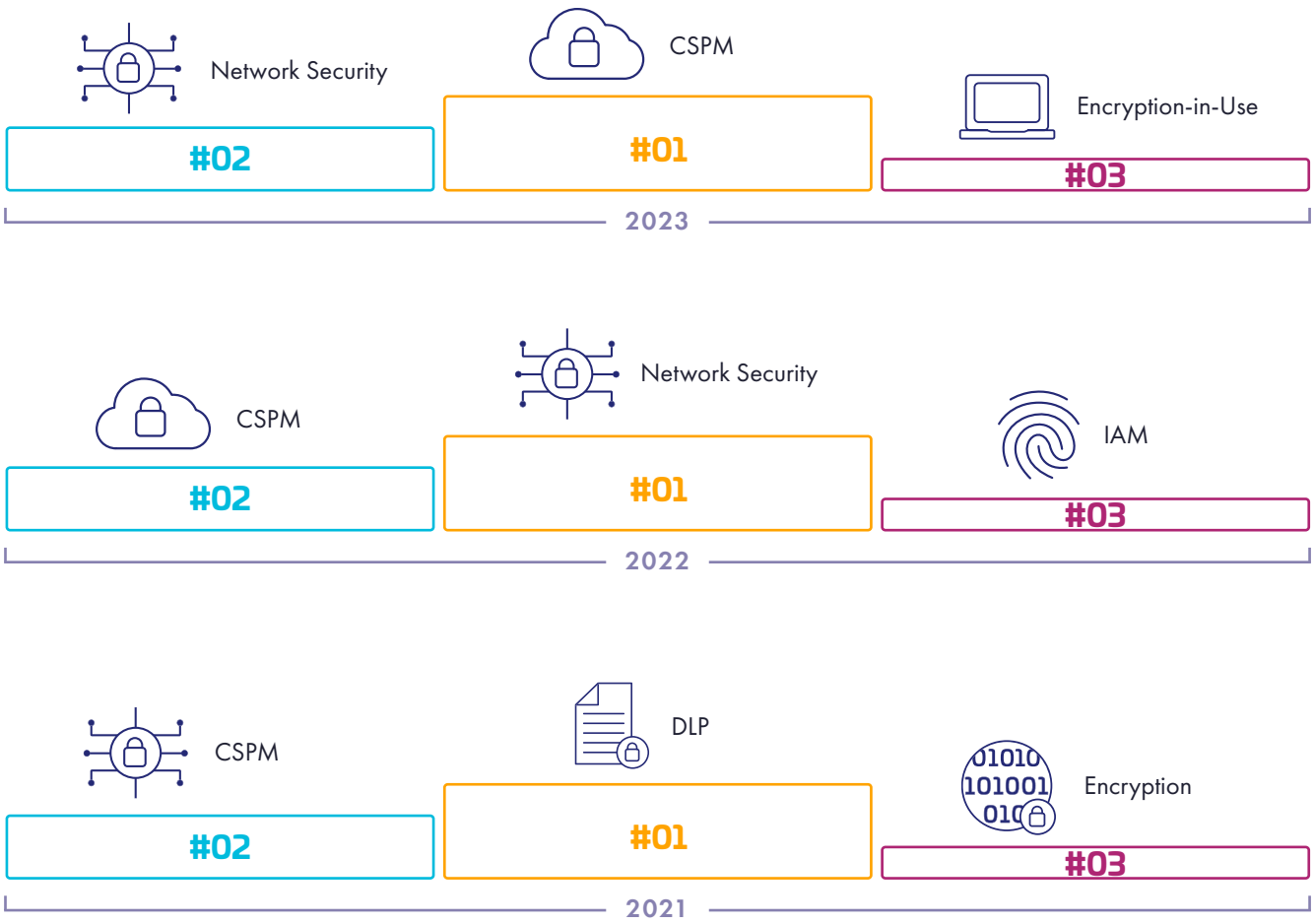
of respondents affected by ransomware say they experienced some data loss from the attack.

Enterprises did report a shift in spending to prevent ransomware attacks. In 2022, 57% of respondents said they would shift or add a budget for ransomware tools, rising to 61% in 2023. Despite these shifts, the response focus remains unclear. When asked what tooling organizations are spending on, responses have been varied.

While enterprises report limited relief from ransomware attacks compared to last year, the results and responses from this year's study still suggest closer stakeholder collaboration. While ransomware attacks are generally characterized by their immediate challenge, other long-term challenges in data security will persist with emerging threats.

Security technologies receiving current spending

Which of the following security technologies are you spending on today?



A new security technology has been added to the 2023 Thales Data Threat Report, "Encryption in use." Encryption-in-use tools are part of a larger set of data-in-use data security enforcements that preserve the utility of data even when data secrecy persists. These emerging products include confidential computing and privacy-enhancing technologies. For more information, please see 451 Research's Data Security Enforcement Market Map 2022.

Post-quantum cryptography — plans and prototypes

Advances in quantum computing and the resulting ability to break classical encryption schemes are an increasing concern. Post-quantum cryptography (PQC) has emerged as a discipline to counter these concerns. Whereas classical encryption schemes such as RSA-2048 may require thousands of years to crack by "brute force" using conventional computing, quantum computing via Schorr's algorithm could potentially crack classical encryption techniques in seconds rather than centuries. Given the ubiquity of classical encryption schemes, the National Institute of Standards and Technology has been steadfastly calling for and collaborating on different PQC algorithms for secure key exchange and digital signatures. In 2022, it vetted four PQC algorithms, which are already being ported into common cryptographic libraries such as OpenSSL.

As such, respondents indicate that future decryption of today's data — or harvest now, decrypt later (HNDL) — and network decryption are their greatest security concerns regarding quantum computing. The concern with HNDL attacks is that adversaries are capturing classically encrypted data only to decrypt it at a more opportune, quantum-ready time. While 62% of respondents said network decryption was the PQC security threat of greatest concern, many enterprises count on legal safe harbors for breach notification if lost data has been encrypted with strong classical controls.

62%

of respondents said network decryption was the PQC security threat of greatest concern.

Given the emerging challenges and solutions, PQC advocates have emphasized the practice of "crypto-agility," whereby cryptography implementations are iterated in their validation and application. Simplification and consolidation, such as reducing the number of key management systems in use, are the best proactive measures enterprises can take to ensure crypto-agility.

For example, 62% of respondents report having five or more key management systems for their enterprise, up from 57% in 2022. Many key management systems can be unwieldy and represent a greater burden for ensuring crypto-agility.

62%

Nearly two-thirds (62%) of enterprises have five or more key management systems, presenting a challenge for PQC and crypto-agility.

Back to basics

After studying both internal attitudes and external expectations, the 2023 Data Threat Report shifts its focus to examine baseline data security program results and compares them to previous years' outcomes. As mentioned previously, enterprises lack confidence in fully locating their data, with 35% of respondents "somewhat" or "not at all" confident for 2021, 2022 and 2023. Similarly, 20% of enterprises have consistently been unable to classify their data across these three years. These figures remain stubbornly high across all geographies, verticals and enterprise sizes.

Perhaps due to increasing regulatory burdens, audit failure remains stubbornly high — though it does show incremental improvement. The percentage of respondents who reported an audit failure was 48%, 43% and 40% respectively for 2021, 2022 and 2023.

While these shortcomings may seem intractable, a path forward might be better achieved with a closer base of collaboration with more stakeholders. Such collaboration might not resemble conventional internal and external partnerships. For example, according to 451 Research's Voice of the Enterprise: Customer Experience & Commerce, Vendor Selection 2022 study, merchants, marketers and customer experience leaders identify data security as the number one inhibitor to growth for their business, cited by 45% of respondents. Collaboration with other stakeholders — consumers, partners, customers and regulators — offers better buy-in to data security. Data security initiatives can originate unconventionally, so new collaboration patterns are required. By enabling all stakeholders to secure data, enterprises can enable a stronger, more flexible baseline of controls for increasingly dynamic markets.

Moving ahead

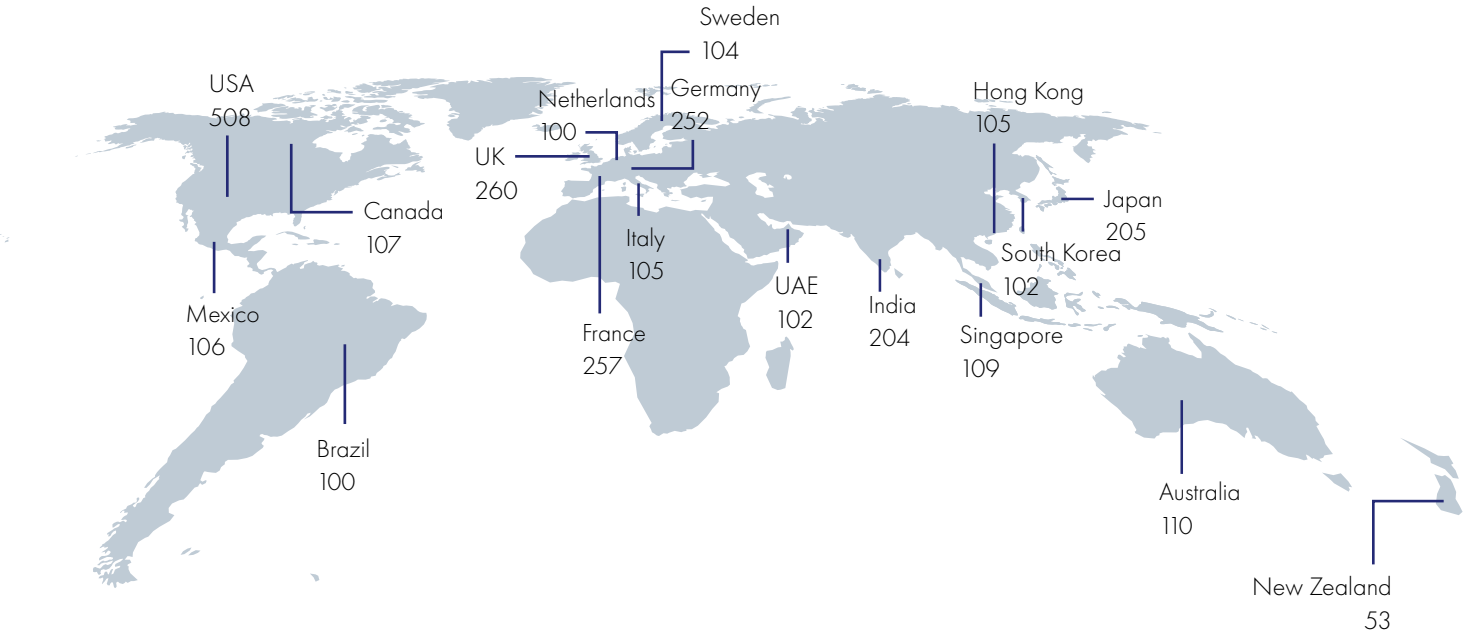
Enterprises face immediate and long-term opportunities for continued growth. As organizations continue their digital transformation to become further data-driven, they need to better collaborate on data security, citizen privacy and digital sovereignty initiatives if they wish to choose their own destiny. Strong data security enables enterprises to adopt new technologies that may serve new markets (such as with 5G/edge) or satisfy internal growth via safe SaaS adoption.

Digital sovereignty represents both a short-term and long-term opportunity for enterprises. While changing data regulations require more immediate responses, long-term data, operational and software independence from any single cloud provider gives the enterprise the foundation to embrace new cloud technologies to strategically grow. Enterprises that maintain more data security controls independent of any single cloud provider can more reliably apply controls to the environment with the best execution value.

It remains imperative for enterprises to better collaborate with their stakeholders. Continued transformation success depends on a greater variety of stakeholders, such as customers, end users, developers, operators, regulators, risk managers and practitioners alike. Understanding their perspectives will allow leadership teams to better navigate the pathways forward.

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.



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/data-threat-report