IDC

Implementing Digital Sovereignty in the Journey to Cloud

Overcoming the Challenges and Complexities of Deploying Sovereignty as Part of a Multicloud Strategy

February 2023

Author:

Archana Venkatraman
Research Director, Cloud Data Management

Rahiel Nasir
Research Director, European Cloud Practice

Ewa Zborowska
Research Director

IDC #EUR149987523

An IDC InfoBrief, Sponsored by

vmware®

Cloud is mainstream, but can we continue on the road as is?

90% of organizations in Europe and 88% in the Middle East, Turkey, and Africa (META) now use cloud technology, which is a keystone for digital transformation.

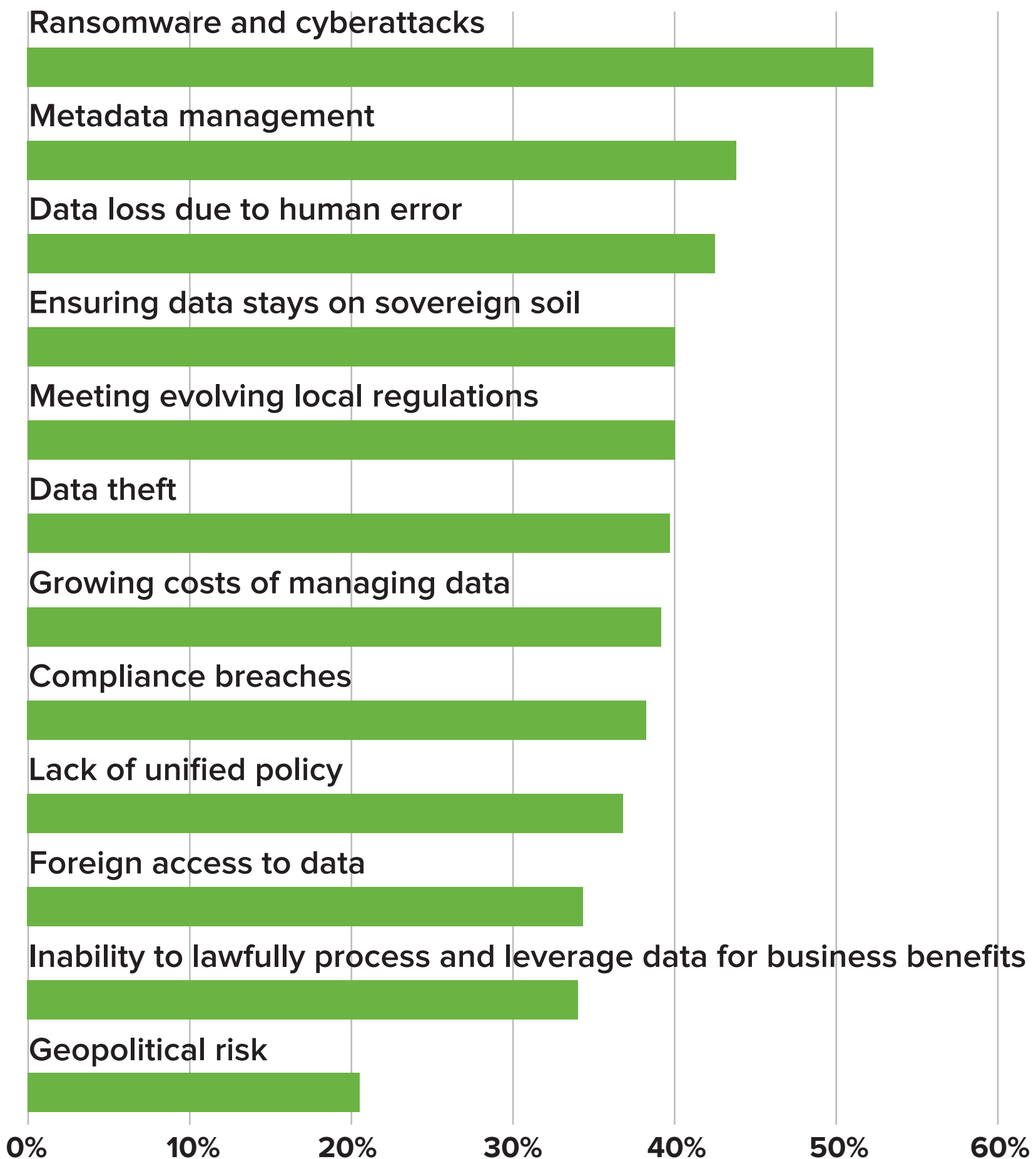As it becomes a dominant IT operating model, critical data is finding its way into the cloud.

Almost 50% of European companies are putting classified data in the public cloud.

While private on-prem cloud remains an organization's primary cloud environment for storing high-sensitivity data, 23% of those surveyed chose public cloud for this data class.

32% of companies use global public cloud providers to store confidential data. This creates challenges related to managing sensitive data and keeping it secure:

Main challenges related to managing sensitive data and keeping it secure.

- Ransomware and cyberattacks
- Metadata management
- Data loss due to human error
- Ensuring data stays on sovereign soil
- Meeting evolving local regulations
- Data theft
- Growing costs of managing data
- Compliance breaches
- Lack of unified policy
- Foreign access to data
- Inability to lawfully process and leverage data for business benefits
- Geopolitical risk

0% 10% 20% 30% 40% 50% 60%

Continuing with current cloud adoption plans is a **risky strategy** because the challenges of managing and securing sensitive data are growing.

Businesses cannot afford to maintain this status quo amid rising sovereignty concerns.
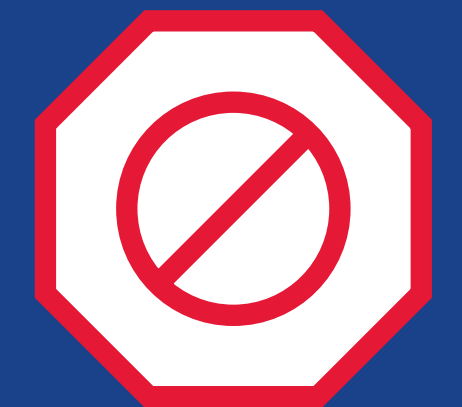
Rising volumes of sensitive data in public cloud make sovereignty an imperative

IDC defines digital sovereignty as the capacity for digital self-determination by nations, companies, or individuals.

Organizations are starting to value strategic autonomy to ensure resilience amid growing geopolitical and economic uncertainties.
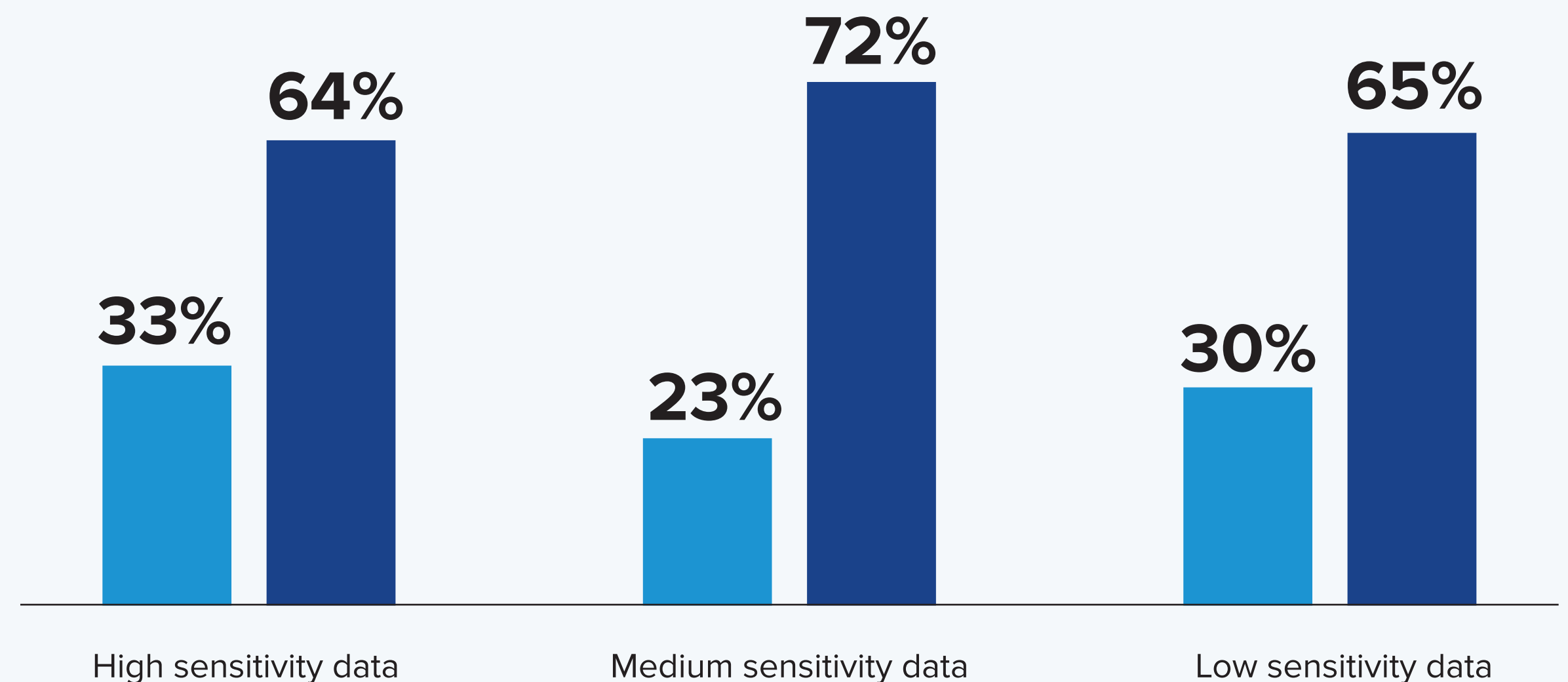
Digital sovereignty starts with data sovereignty, which forms the legal basis for organizations to ensure regulatory compliance. Data sovereignty is about making sure that data is subject to the laws and governance structures of the country it belongs to.

With a large amount of sensitive data now hosted in cloud, sovereignty should influence an organization's future cloud strategy. This is becoming a priority as sensitive data volumes are growing exponentially.

64% of organizations have **increased** their volume of **highly sensitive** data.

Over the past two years, how did the following data types increase or decrease in volume?

● Stayed the same ● Increased

	High sensitivity data	Medium sensitivity data	Low sensitivity data
Stayed the same	33%	23%	30%
Increased	64%	72%	65%

The importance of sovereignty for **EMEA organizations**

The nuances brought by regional, organizational size, and vertical dimensions

The only option for customers to get the sovereign cloud security is to engage with a Cloud Providers which are well positioned in local markets.
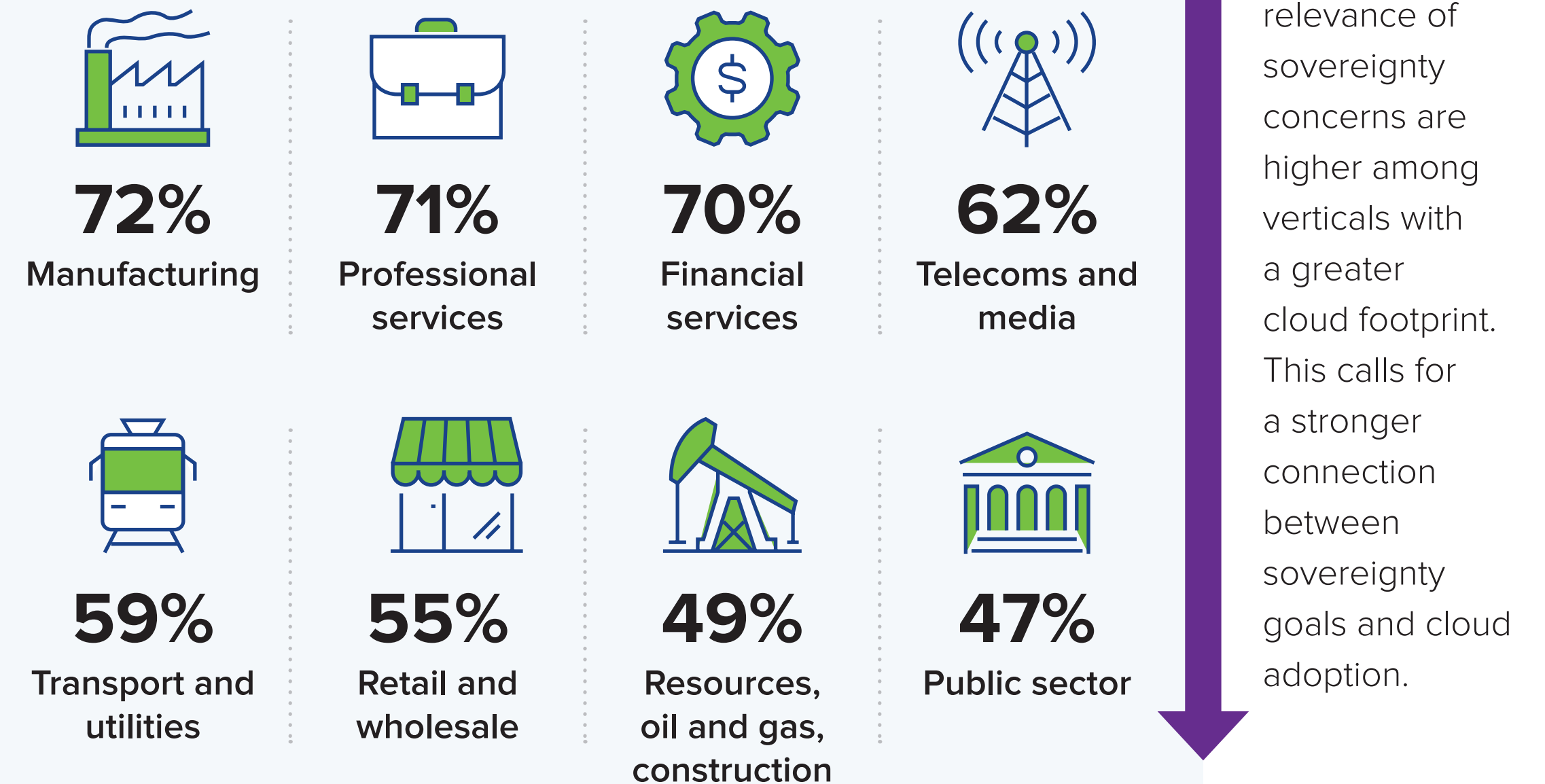
Drivers for considering sovereignty

- Relevance of data sovereignty cited as "very important" or "extremely important" by 88% of very large organizations (5,000 FTEs) and 63% of all EMEA organizations.

- In Europe, organizations are driven by the need for continuous compliance, regulations, and legal obligations.

- In META, organizations are driven by the introduction of internal/corporate policies.

Business drivers for data sovereignty

- Customer expectations about privacy and confidentiality

- Need to protect future investments in data

- Continued macroeconomic volatility, ambiguity, and uncertainties are heightening interest in sovereign solutions

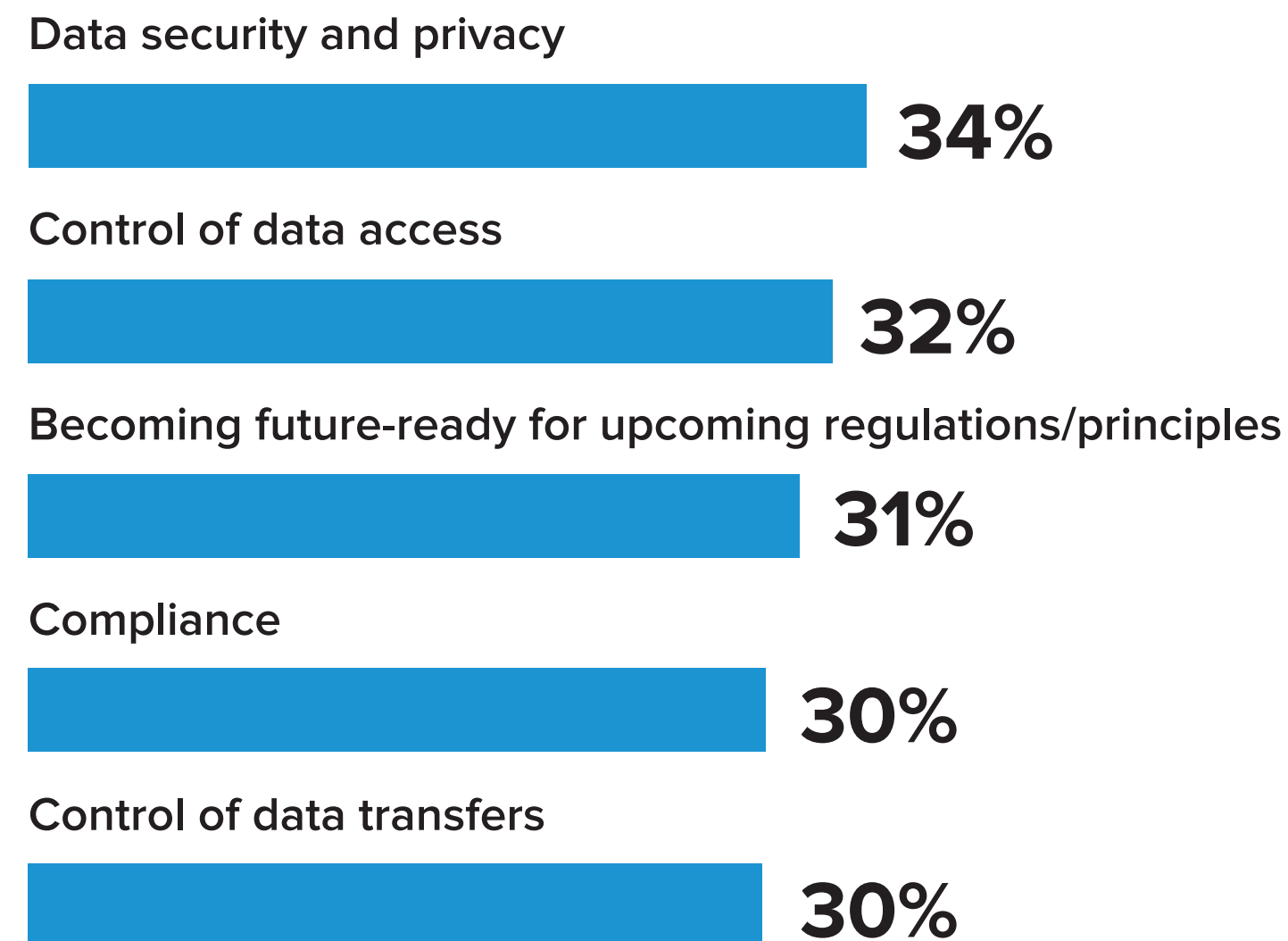- Protection against future EU ruling that could impact your business

How different industry verticals rate data sovereignty as relevant and important:

72% Manufacturing	**71%** Professional services	**70%** Financial services	**62%** Telecoms and media
59% Transport and utilities	**55%** Retail and wholesale	**49%** Resources, oil and gas, construction	**47%** Public sector

Perceptions about the relevance of sovereignty concerns are higher among verticals with a greater cloud footprint. This calls for a stronger connection between sovereignty goals and cloud adoption.
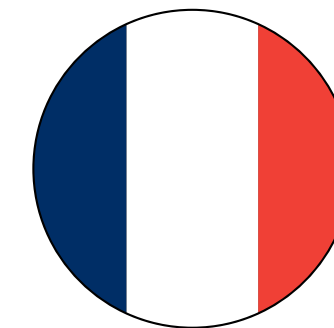
The benefits of adopting a sovereign cloud vary by country

Around 60% of organizations across Europe and the META region consider data sovereignty to be strategic or very important for their cloud strategies.

Data sovereignty components are among the top 5 benefits companies expect from sovereign cloud ...

Data security and privacy

34%

Control of data access

32%

Becoming future-ready for upcoming regulations/principles

31%

Compliance

30%

Control of data transfers

30%

... but not all markets are equal and the top benefits can vary by country:

French organizations want to become future-ready for data-driven business innovation.
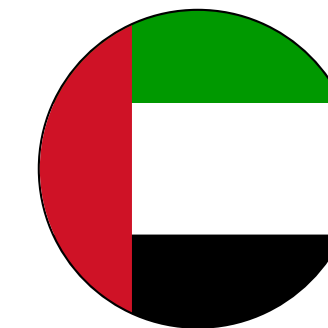
Meeting compliance requirements is the top benefit of a sovereign cloud for organizations in UAE.

Those in Germany expect sovereign cloud to help them become future-ready for upcoming regulations and new principles.

In the U.K., organizations want control of data transfers.

Benefits of sovereign cloud are plentiful but organizations need help to navigate the complexities

Growing **complexity** of IT platforms leads to greater demand for partners and providers that offer **flexibility**, **independence**, and **control**.

29% are looking for partners that offer greater flexibility and choice.

Gaining freedom from vendor lock-in is a top requirement for 29%.

23% want to leverage a strong ecosystem when using a sovereign cloud platform.

Expected benefits vary depending on an organization's approach to digital sovereignty:

Companies with implemented data sovereignty strategies look for:

- Flexibility and choice
- Data security and privacy
- Compliance

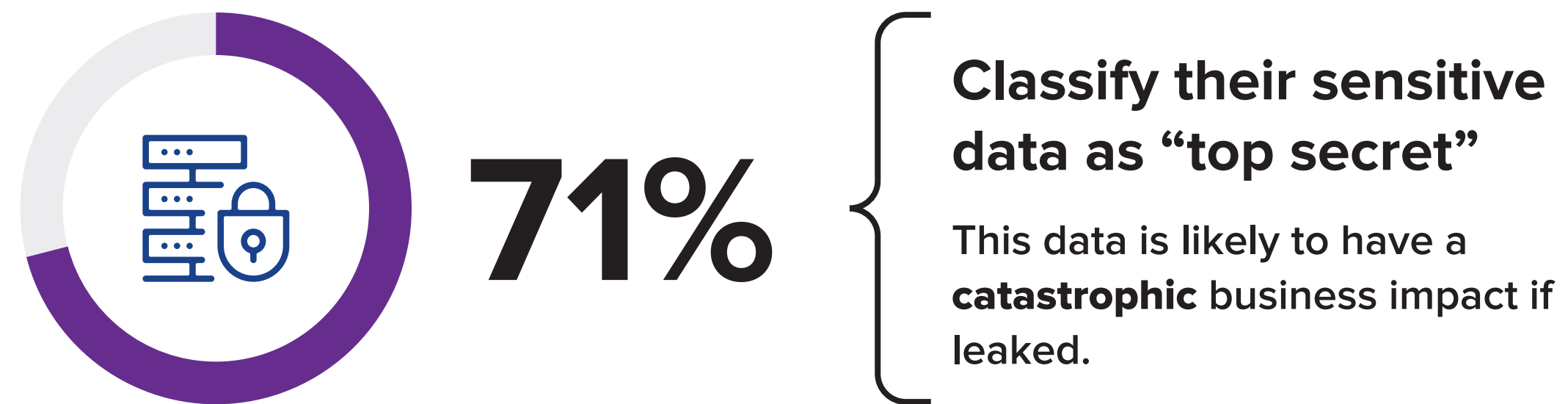Companies that see data sovereignty as strategic look at:

- Data security and privacy
- Control of data transfers
- Becoming future-ready for upcoming regulations/principles
- Cloud providers' skills

Whatever short-term benefits are expected, the goal for companies is for digital sovereignty to result in enhanced customer, government, and stakeholder trust in their organization and greater business resilience.

How organizations are classifying their data

Organizations trust cloud and keep a significant portion of their classified and sensitive data in various environments, including public cloud, private cloud, and colocation facilities, as well as on premises.

71%

Classify their sensitive data as "top secret"

This data is likely to have a **catastrophic** business impact if leaked.

62% of organizations say their current cloud use does not fully meet their data sovereignty requirements.

More than half of organizations say they require sovereign capabilities for up to 10% of their data kept in the cloud.

That means for **90%** of data kept in the cloud there remains the vital need for organizations to review their security and compliance processes, tools, and skills, as there might be an unmet demand for sovereignty solutions that they are not aware of.
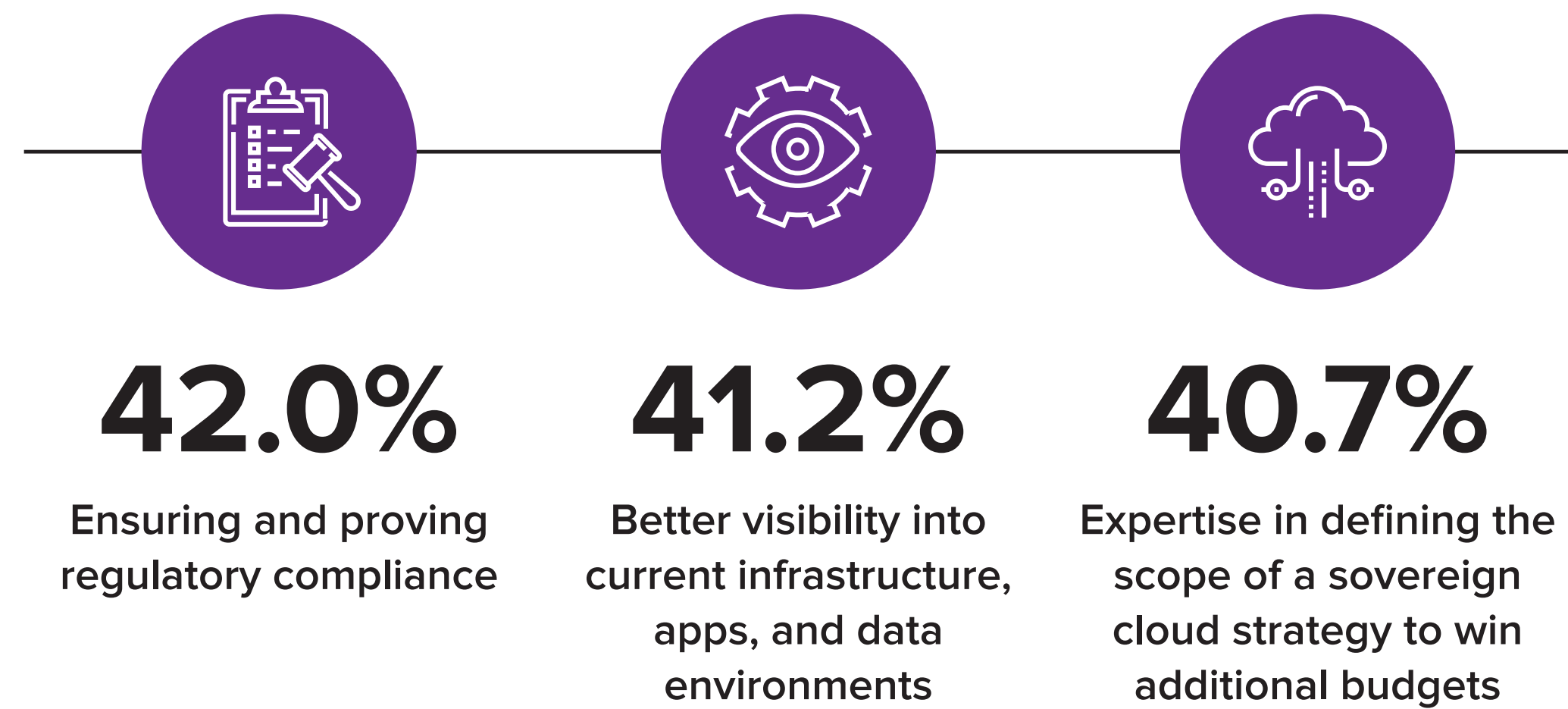
What organizations need to deploy sovereign solutions

As companies realize the key role of partners in deploying sovereign solutions, a **trusted brand** becomes the number 1 non-technical attribute organizations look for when seeking sovereign cloud partners.

End-to-end capabilities and certifications will also be crucial when choosing a partner for a sovereign solution deployment.

The top 3 **capabilities** organizations seek to manage sovereign clouds:

42.0%
Ensuring and proving regulatory compliance

41.2%
Better visibility into current infrastructure, apps, and data environments

40.7%
Expertise in defining the scope of a sovereign cloud strategy to win additional budgets

IDC research shows that cybersecurity and governance are top priorities for companies.

For sovereign solutions, security and compliance must be maintained on an ongoing basis and as a shared responsibility between vendor and customer.
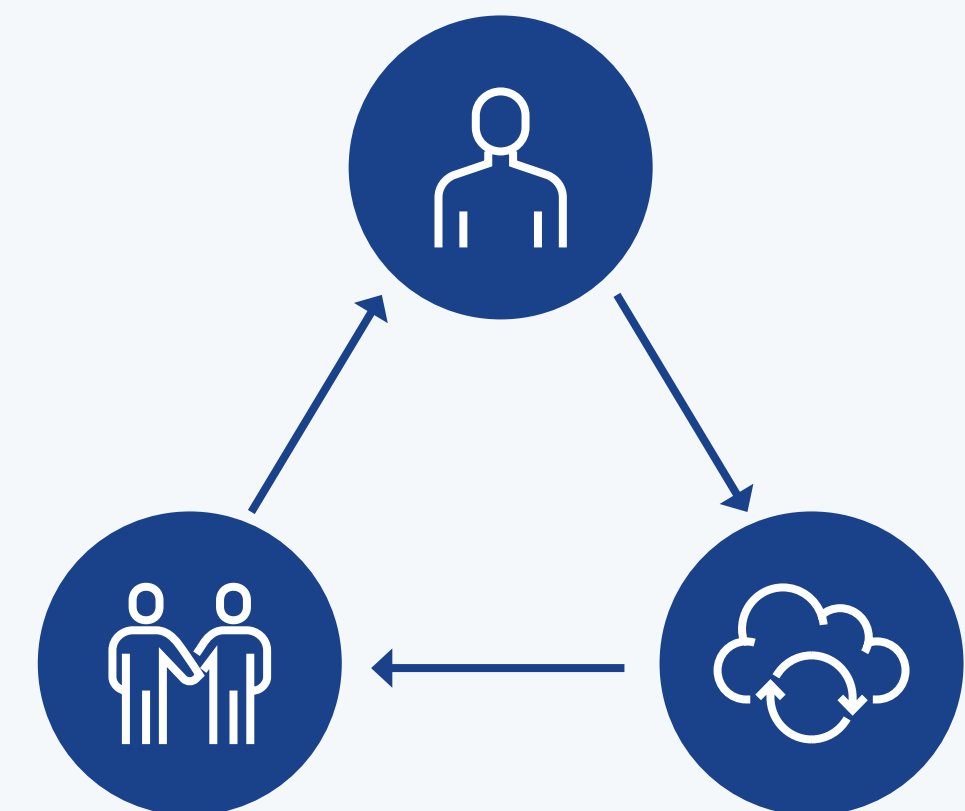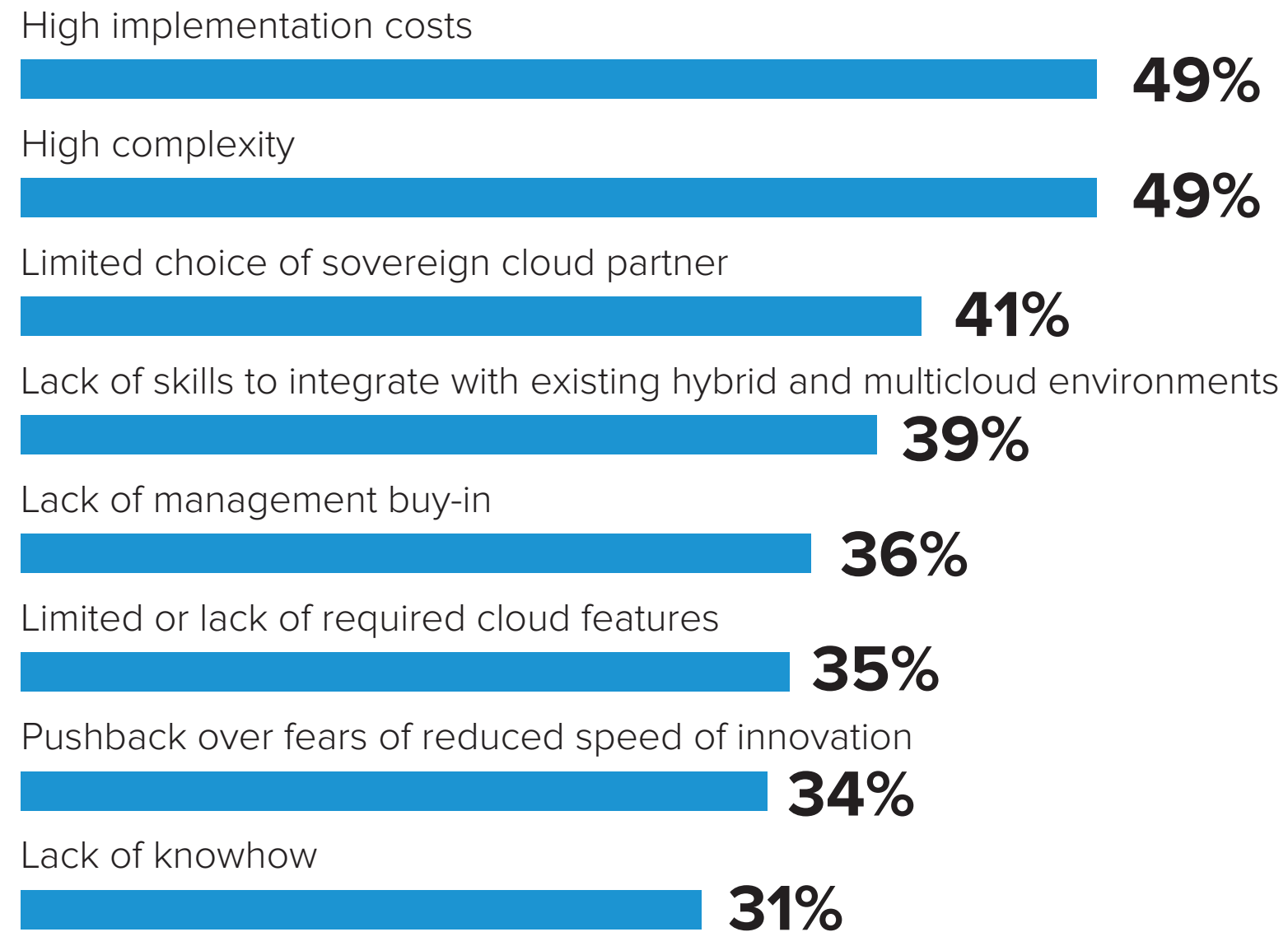
It is therefore essential to work with partners that can verify trusted credentials.

Sovereign cloud is not a "done deal" — most organizations face deployment challenges

Despite many organizations using public cloud for their "top secret" and "highly confidential" data, only 19% have actually implemented a sovereignty strategy.

When asked about their main concerns regarding implementing a sovereign cloud strategy, a limited choice of sovereign cloud partners, a lack of skills to integrate solutions into existing cloud environments, and a limited range of cloud features were among the challenges cited:

High implementation costs
49%

High complexity
49%

Limited choice of sovereign cloud partner
41%

Lack of skills to integrate with existing hybrid and multicloud environments
39%

Lack of management buy-in
36%

Limited or lack of required cloud features
35%

Pushback over fears of reduced speed of innovation
34%

Lack of knowhow
31%

How much for a sovereign cloud?

53%

40% of organizations anticipate increasing their investment in sovereignty solutions over the next two years. This rises to 53% over a longer term of three to five years.
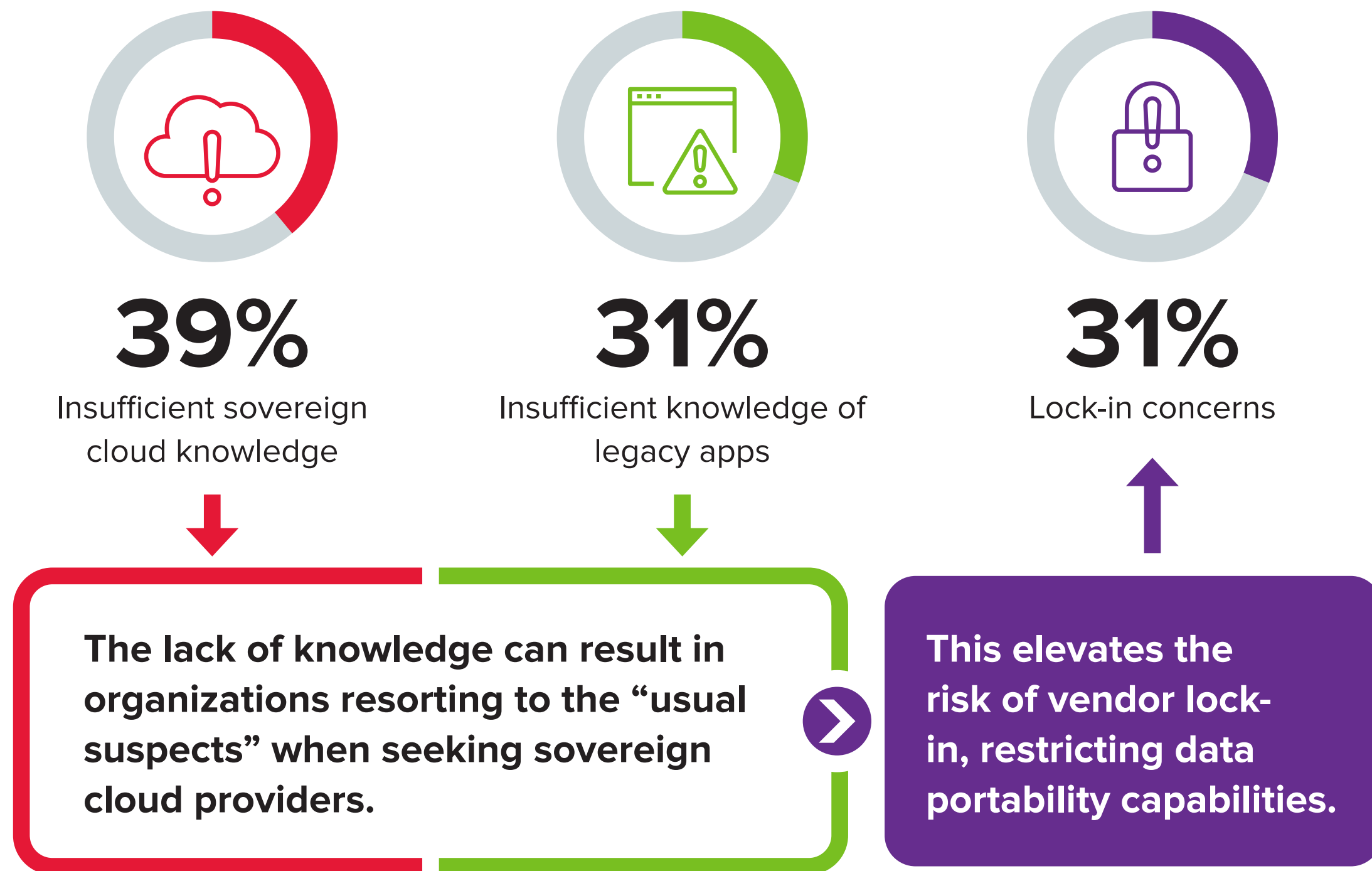
30%

Just under half are willing to pay up to 10% more for sovereign cloud offerings, but larger firms with 1,000 or more employees are prepared to pay as much 30% extra.

39%
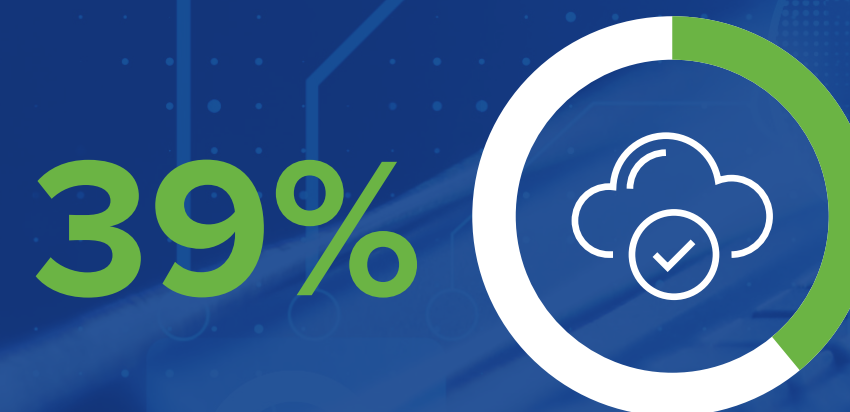
However, 39% remain reluctant to pay any premiums for such solutions. This unwillingness suggests a need to embed sovereignty into cloud solutions by default.

Top challenges of moving workloads to sovereign cloud reveal lack of maturity:

39%

Insufficient sovereign cloud knowledge

31%

Insufficient knowledge of legacy apps

31%

Lock-in concerns

The lack of knowledge can result in organizations resorting to the "usual suspects" when seeking sovereign cloud providers.

This elevates the risk of vendor lock-in, restricting data portability capabilities.

A limited choice of sovereign cloud providers is one of the top concerns for 41% of organizations implementing a sovereign cloud strategy.

Pitfalls to avoid

Maintain balance
Sovereign solutions are by nature restrictive. Organizations must balance their needs so as not to stifle business innovation.

Trusted partnerships and support are vital
Sovereignty cannot succeed in a vacuum. Organizations will need to work with an ecosystem of partners and providers as part of a multisourced, multicloud strategy.
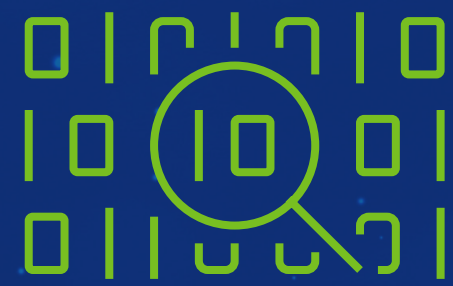
Full-service clouds
Local cloud providers can offer highly secured capabilities for secret and confidential data. Hyperscalers can complement with advanced innovation features for protected data.

Building the foundations to implement sovereignty

Preparing for sovereignty

Data discovery and classification

This is essential for any data governance, privacy, and security program. The process helps to build an understanding of what types of data are held, how it flows through the organization, and what the most suitable venues are for each workload and app.

Security is a shared responsibility

It's vital to maintain cybersecurity and regulatory compliance on an ongoing basis. Crucially, this must be a shared responsibility between all partners. Customers and their partner providers must work hand in hand throughout the entire process of deploying and operating a sovereign solution.

Tool up and skill up

A sovereign cloud needs to fit into an organization's multicloud or hybrid strategy. This may require additional investments in new tools for data governance and management, redesigning internal processes to ensure compliance, and new skills to support all this. New infrastructure and platforms will also be needed.
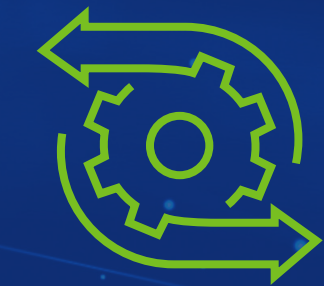
Sovereign today, sovereign tomorrow

Implementing sovereignty principles is a long-term process. It involves adapting to new IT requirements in terms of infrastructure, strategy, governance framework, and skills. All stakeholders must continually monitor all new and upcoming legislation and regulations that will impact their sovereign status and plan accordingly.

Building the foundations to implement sovereignty

Choose the right partners and providers to meet your strategy

Flexibility is essential

Because of all the costs, complexities, and processes involved, customers should seek out partners and providers that offer the greatest adaptability, flexibility, and control for customers looking for sovereign solutions.

Beware of vendor lock-in

Solutions that lead to vendor lock-in will restrict data maneuverability for customers. Open source solutions lend themselves well to data interoperability, portability, and transferability. This is vital for sovereignty success.

Cross-examine the provider

Vendors should be prepared for greater customer and auditor scrutiny. Organizations should therefore look for providers that offer the greatest transparency in terms of their solutions, services, and platforms. Working within an ecosystem is also a foundation for sovereignty success, but customers must seek assurances that all the provider partners adhere to sovereign rules. Cloud providers are able to support customer needs.

Trust and resilience

Choose a trusted provider that can demonstrate key sovereign capabilities, offer a broad level of expertise and skill sets, and engage all the main stakeholders and lines of business in the user organization. Ultimately, digital sovereignty should be seen by both providers and customers as way of helping organizations to become more resilient.

Message from the sponsor

Sovereign Cloud is all about choice and control. VMware's offering addresses the strategic imperatives for data sovereignty on data security, protection, residency, interoperability, and portability:

- Leveraging the VMware Multicloud Foundation
- Innovating on sovereign capabilities (Tanzu, Aria, open ecosystem solutions)
- Leveraging a broad ecosystem of sovereign cloud providers

VMware is well recognized on trust and on several capabilities for data sovereignty needs: flexibility and choice/data security and privacy/control of data access/multicloud/ data residency. It is already deployed with more than 20 Sovereign Cloud Providers.

"To ensure success in their sovereign journey, organizations must work with partners they trust and that are capable of hosting authentic and autonomous sovereign cloud platforms. VMware Cloud Providers recognized within the VMware Sovereign Cloud initiative commit to designing and operating cloud solutions based on modern, software-defined architectures that embody key principles and best practices for data sovereignty. More than 36 global and 14 EU VMware Sovereign Cloud Partners can deliver to customers cloud services in alignment with security and local regulations, while enabling sovereign innovation." **Laurent Allard, Head of Sovereign Cloud, VMware**

To learn more, please visit
https://cloud.vmware.com/providers/sovereign-cloud

vmware®

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Corporate Headquarters
140 Kendrick Street,
Building B, Needham,
MA 02494 USA
508.872.8200
www.idc.com