

Digital Sovereignty in Action: Building Resilient, Compliant, and Transparent Cloud Ecosystems

An Executive Guide to digital control in a cloud-driven world



Ewa Zborowska,
Research Director,
AI, Europe



Rahiel Nasir,
Research Director,
European Cloud Practice

Table of Contents

Executive Summary	3
Defining Digital Sovereignty — IDC’s Digital Sovereignty “Stack”	4
Building a Sovereign Cloud — IDC’s Sovereign Cloud Taxonomy	5
Who Is Using Sovereign Cloud Solutions and Why?	6
Using Sovereign Cloud	7
Benefits of Sovereign Cloud	8
AI Workloads and Digital Sovereignty	9
Ensuring AI Sovereignty	11
Master Challenges of Sovereign Cloud	12
Digital Sovereignty Success — Choosing Partners with Expertise	13
Digital Sovereignty Success — Choosing the Right Partner	14
Digital Sovereignty Success — Working Within Sovereign Ecosystems	15
Vivicta	16
Recommendations for Clients	17
About the Analysts	18
Message from the Sponsor	19
About IDC	20

Executive Summary

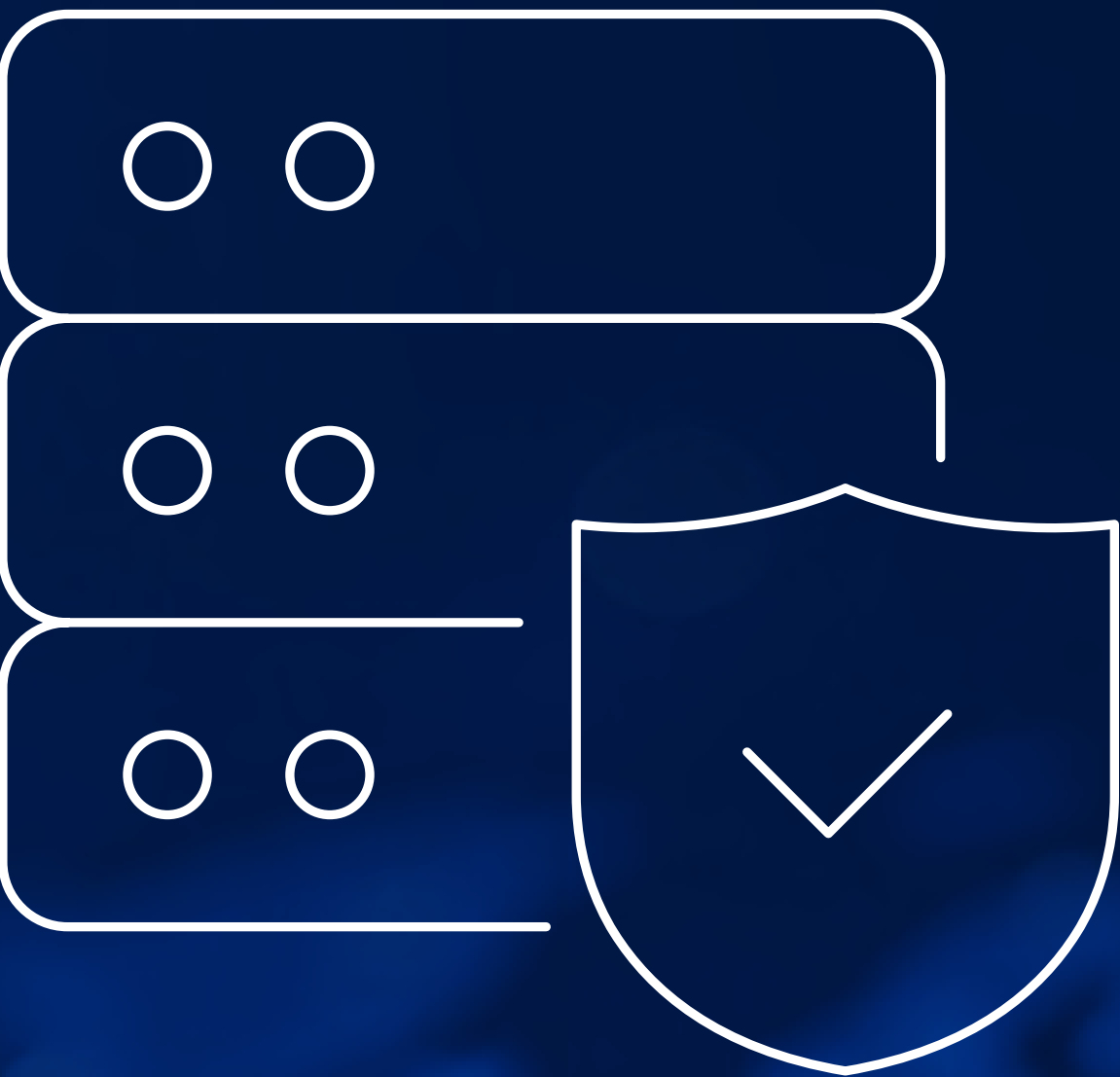
As digital technologies continue to advance, concerns around data privacy and control have driven the emergence of digital sovereignty, a concept that empowers governments, organizations, and individuals with greater control over their data.

This concept is initially built on the foundation of data sovereignty, which includes IT solutions that ensure the proper management and compliance of data from collection through storage. As the use of cloud and digital technologies continues to increase, digital sovereignty also encompasses technical and operational sovereignty, focusing on infrastructure and operational transparency, enabling greater resilience and security for critical infrastructure. Cloud is at the center of digital sovereignty developments, and interest in sovereign cloud solutions is growing, particularly in Europe. Key drivers for this include the need to enhance cybersecurity, expand cloud use, and ensure regulatory compliance. Furthermore, as AI adoption accelerates, ensuring AI workloads align with digital sovereignty principles is critical to balancing innovation and data governance.

However, challenges such as high complexity, skills gaps, and rising costs remain significant barriers. Organizations also face difficulties in terms of integrating sovereign cloud solutions into their existing IT environments, ensuring long-term compliance, and preventing vendor lock-in.

To overcome these challenges, organizations are seeking trusted partners who can offer expertise in data management, cybersecurity, and data classification, while also providing support in navigating the evolving regulatory landscape.

Ultimately, digital sovereignty enables organizations to maintain control over their data, protect against external interference, and ensure security, resilience, and compliance, positioning them to stay competitive in an increasingly data-driven world.



Defining Digital Sovereignty — IDC’s Digital Sovereignty “Stack”

As the use of digital technologies continues to increase, so do concerns around data privacy and data control.

This has led to the concept of digital sovereignty. This is a broad concept that comprises various attributes aimed at giving governments, organizations, and individuals the capacity for digital self-determination.

Essentially, digital sovereignty gives companies greater control of their data and where it resides. It also means greater operational resilience, which is especially crucial for governments who want to ensure critical national infrastructure is always available.

The journey to digital sovereignty begins with data sovereignty. This should include technology solutions that provide a holistic view of how data are collected, classified, processed and stored — and then also managed and monitored, to ensure that regulations are always being met.

It is vital to ensure that sovereign controls to protect data are applied to both data at rest and in transit.



GEOPOLITICAL



Economic; trade dependence;
military



SUPPLY CHAIN



Chip manufacture; raw materials;
energy; skills



ASSURANCE



Assured workloads; business continuity &
disaster recovery; redundancy; portability



OPERATIONAL



Controls & stability; authorized key
access for customer, admin & support



TECHNICAL



Protectionism; interoperability;
portability



DATA



Regulation; portability;
data transfers



Building a Sovereign Cloud — IDC’s Sovereign Cloud Taxonomy

The Three Primary Technology Markets for Digital Sovereignty

1

As well as solutions for **data sovereignty**, organizations also need those that offer controls for technical sovereignty. This refers to all the digital infrastructure, including the datacenters, IT hardware, software, and XaaS used for cloud-based data and workloads. All of that should be shielded from extra-territorial interference, which may prove difficult if the vendors that provide all the assets are foreign firms.



2

Technical sovereignty should also include open-source solutions that lend themselves well to data interoperability, portability, and transferability, as organizations can not afford to lock themselves into custom-built solutions that become legacy systems in their own right.



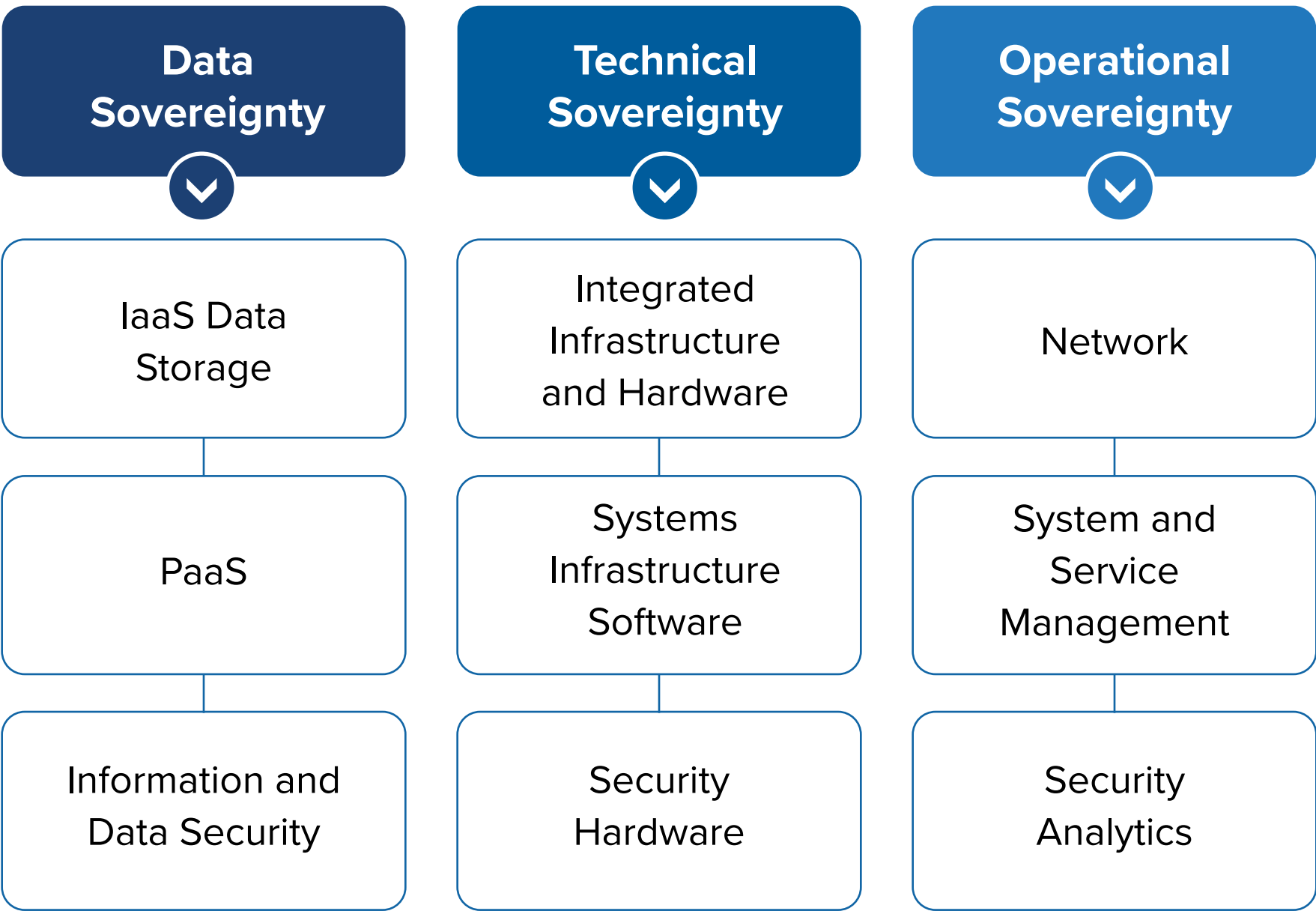
3

A third aspect to building a sovereign cloud is **operational sovereignty**. Here, technology providers should offer cloud capabilities that enable transparency in controlling operations, from provisioning and performance management to monitoring physical and digital access to the infrastructure.





Ultimately, digital sovereignty is about control for the data owner, and that includes control over all aspects of software used for data in a sovereign cloud, as well all the underlying infrastructure and hardware that supports that.



Source: IDC’s Worldwide Sovereign Cloud Taxonomy, 2024

Cloud will be at the center of digital sovereignty developments.



One size does not fit all, and organizations must choose the most appropriate venues for their workloads, especially as true sovereign control of every aspect of the cloud stack may not be possible.

Who Is Using Sovereign Cloud Solutions and Why?

In 2024, 31% of European organizations surveyed said they are currently using sovereign cloud solutions, while 50% plan to do so in 2025.

The **top three European countries** in which organizations are planning cloud usage in 2025 are Austria (64%), Italy (60%), and in joint third place, Czech Republic and Poland (54% each).

The **top three industry sectors** in Europe planning to use sovereign cloud solutions in 2025 are manufacturing (58%), education (54%), and in joint third place, transportation & leisure and finance (51% each).

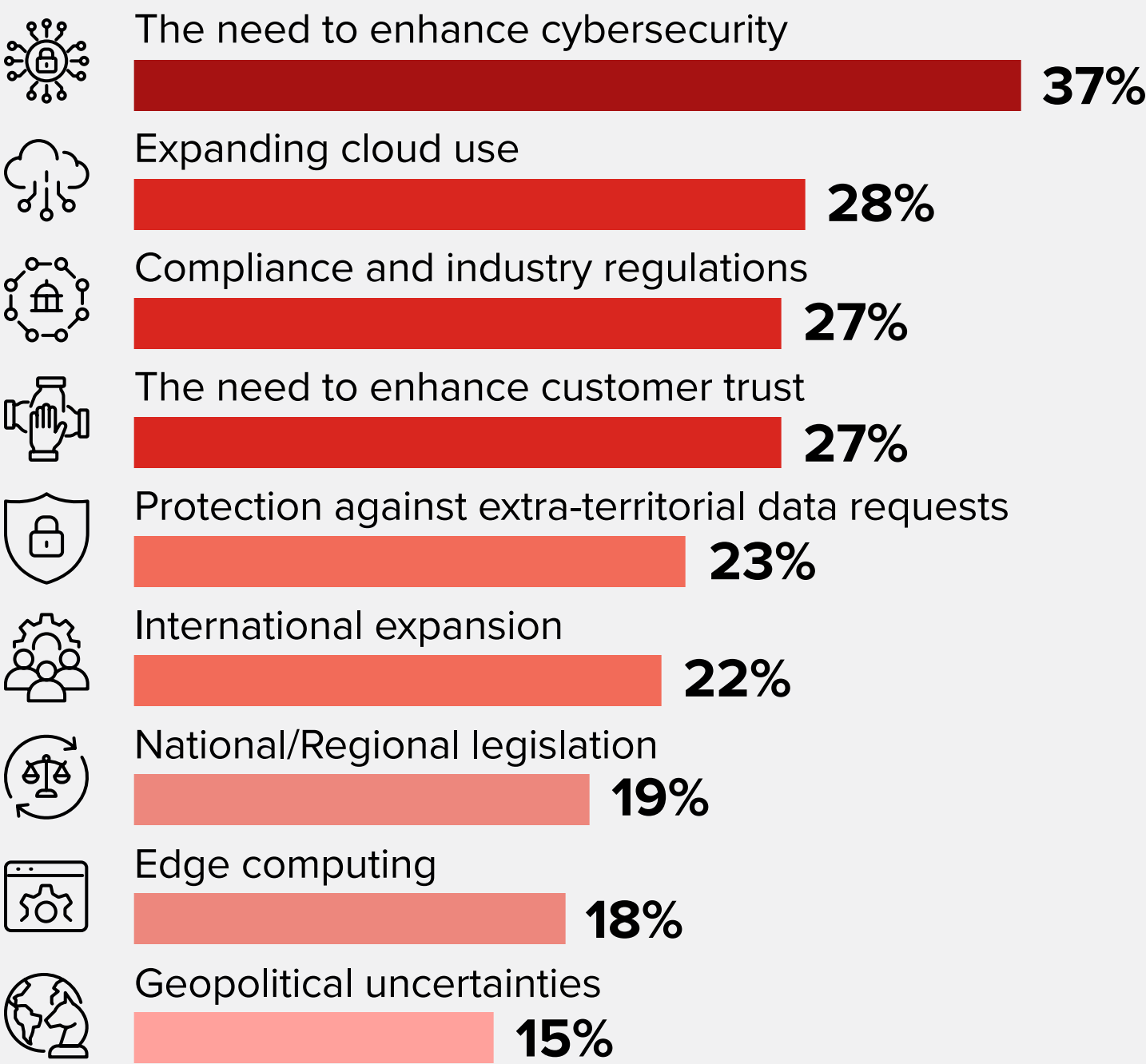
Many organizations across Europe are still at the early stages of their cloud migration strategies. As they begin their digital transformations, these organizations and those in other countries are considering everything they will need for cloud, including solutions for sovereignty.

The top three market drivers for utilizing sovereign cloud are the need to enhance cybersecurity (37%), expanding cloud use (28%), and compliance & industry regulations (27%).

While all companies regardless of size selected the need to enhance cybersecurity as their top driver, there were some variations for the second and/or third driver. For instance, smaller organizations (with 100-499 employees) chose the need to enhance customer trust as their second biggest driver (28%), while 25% of those with 500-999 employees said international expansion was one of their top three drivers.



What's driving sovereign cloud use?



In 2024, only 15% of organizations cited geopolitical uncertainties as their top driver for using sovereign cloud. But given the rapidly changing political climate so far witnessed in 2025, many organizations now have heightened concerns around trust when it comes to choosing and using technology vendors and partners.

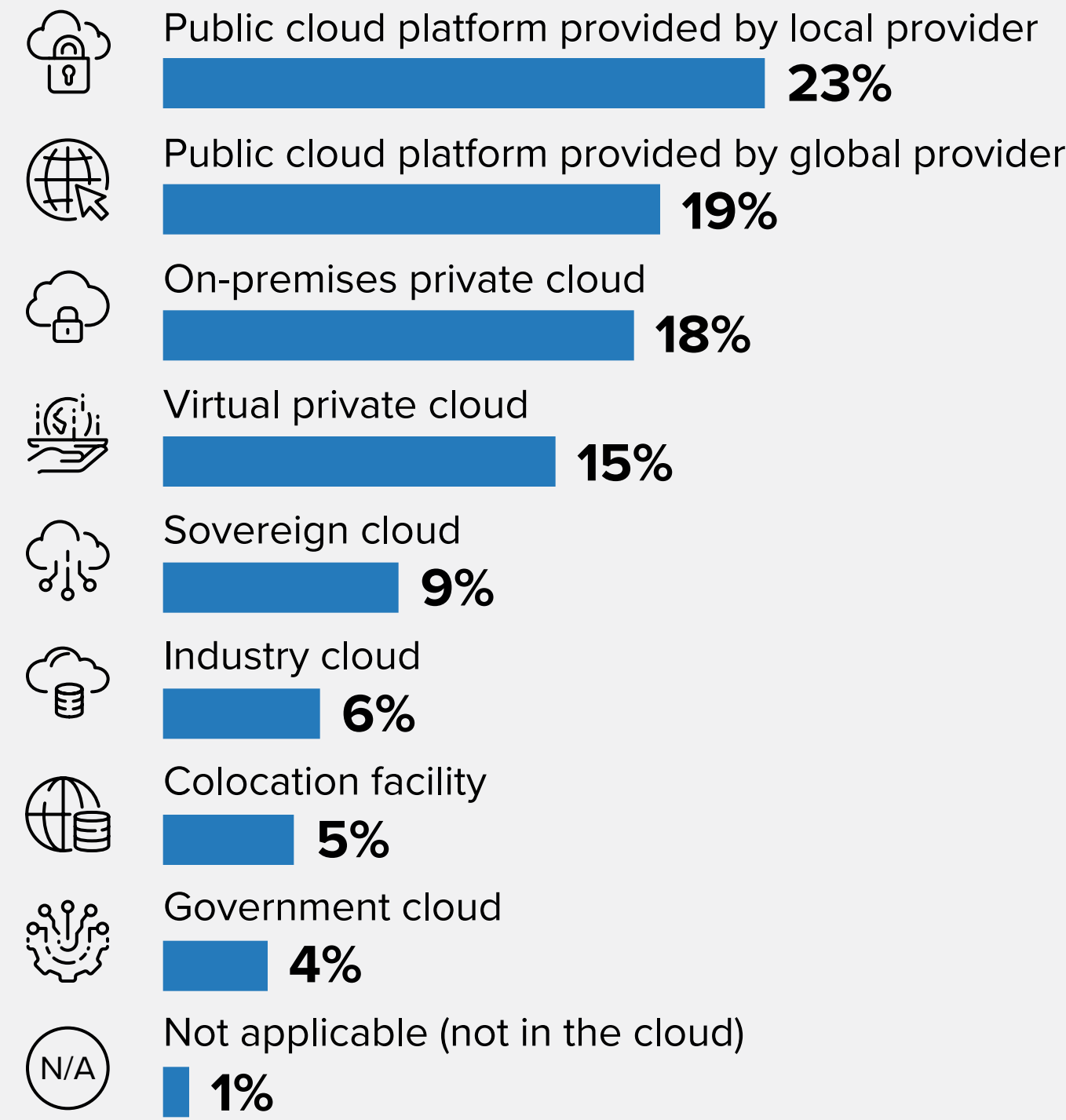
Using Sovereign Cloud



The top workloads migrated to a sovereign cloud by organizations in Europe include data management (38%), storage (36%), and back-up/recovery (35%).

- Deciding which workloads need sovereign control will be determined by the local regulations and legislation that apply to the jurisdictions in which organizations operate. Then comes the complex process of reviewing and classifying data and workloads according to sensitivity needs.
- 40% of organizations in Europe say they have data that can be classified as being of “high sensitivity” — that means top secret or highly confidential data. Leakage of such data would have catastrophic impacts on business.
- 24% said they had “medium sensitivity” data; if leaked, it would have a serious impact on business.
- Only 9% of these organizations are using sovereign cloud for their sensitive data. This is often due to a lack of market education in terms of the need for sovereignty, a perceived lack of solutions and providers, as well as challenges such as a lack of skills needed to implement and operate solutions for digital sovereignty.
- This represents an opportunity for sovereign cloud providers to help organizations understand what solutions they offer and how these support the need for sovereignty; they should then also provide the expertise needed to store the right data in the right venue.

What is the primary cloud environment your organization currently uses or plans to use to store sensitive data?



Benefits of Sovereign Cloud

Implementing solutions for digital sovereignty potentially offers unique benefits.

Control of data transfers is regarded as the top benefit by 53% of organizations in Europe, while 46% also cite control of data access.

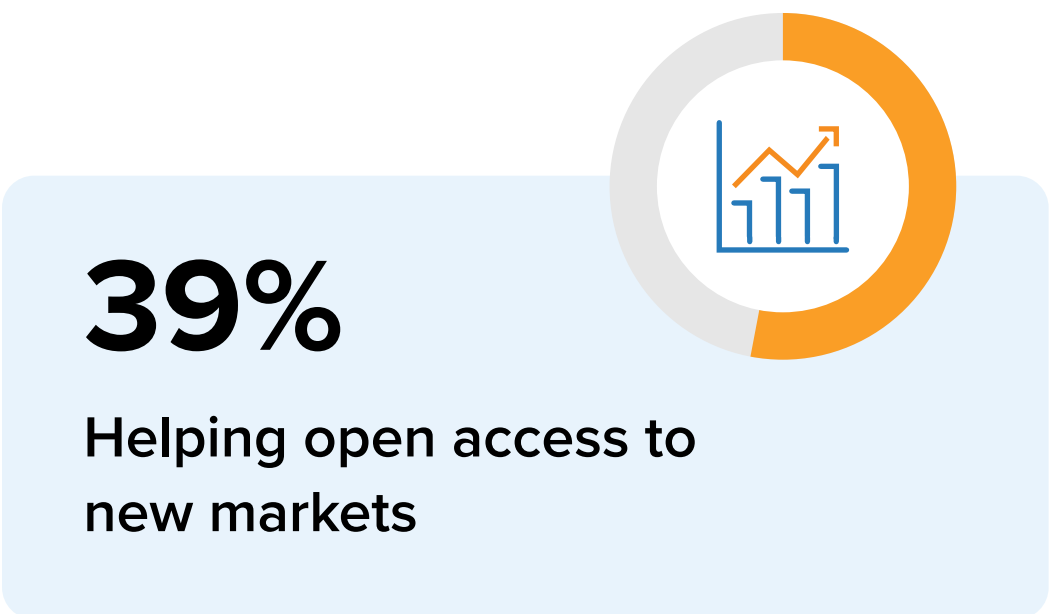
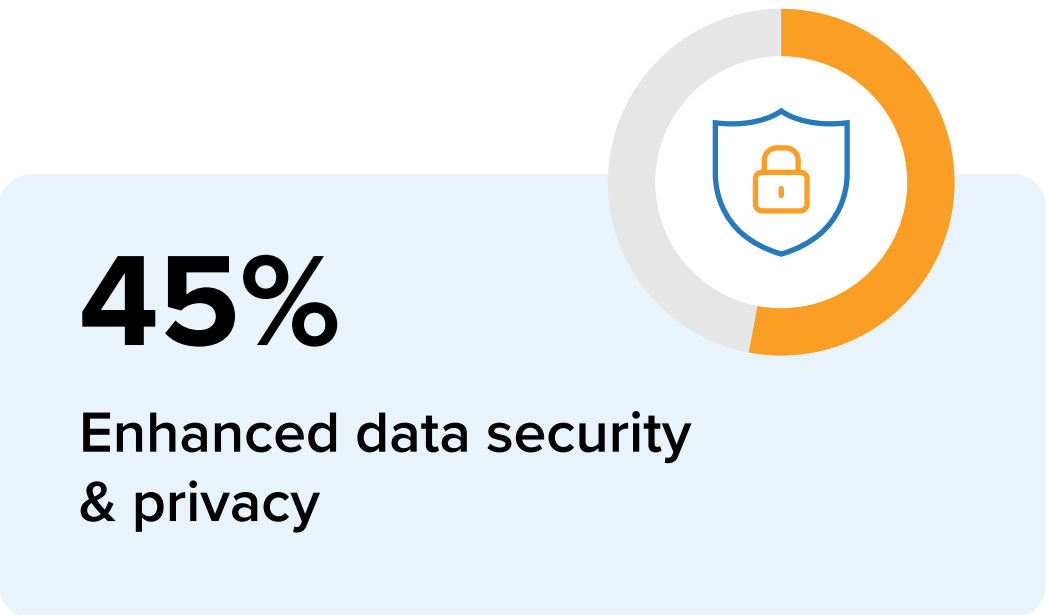
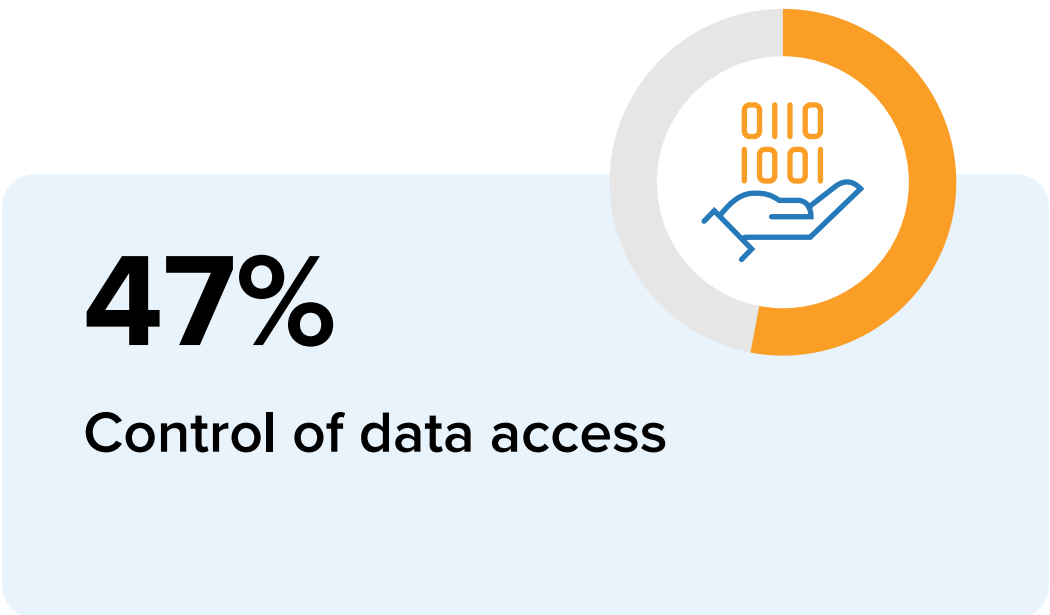
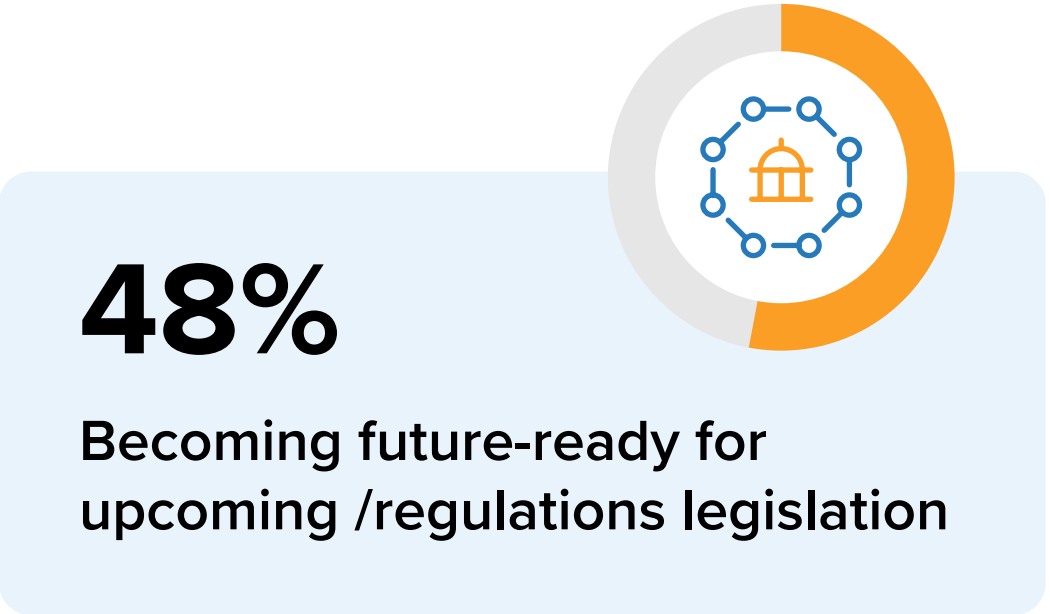
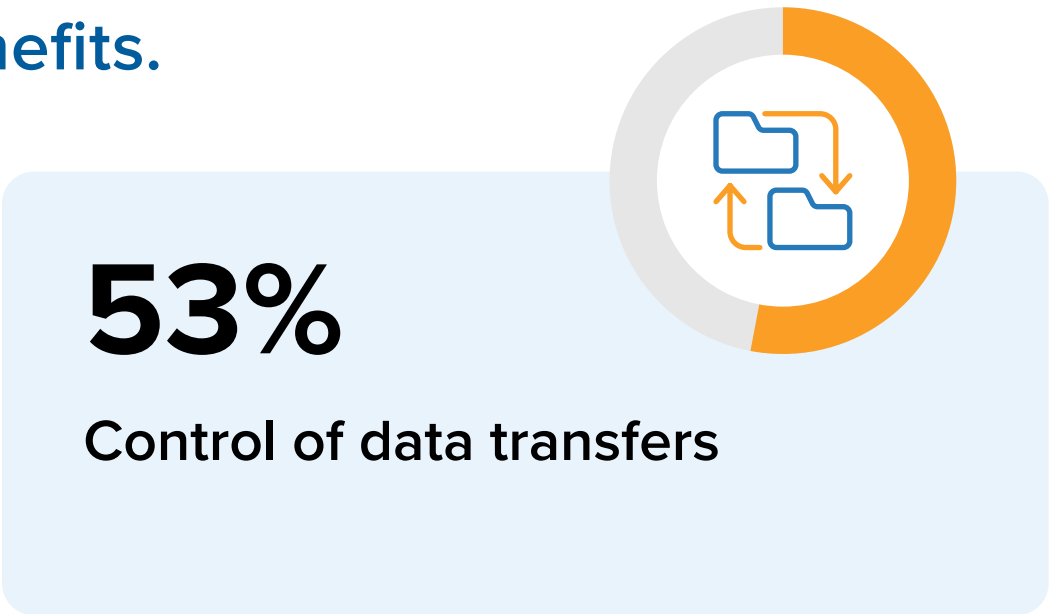
Becoming future-ready for upcoming regulations/legislation is seen as the second main benefit by 48%. This is especially crucial in Europe where the ever-changing regulatory and legislative landscape compels organizations to constantly keep an eye on what is required for sovereignty. They may not need necessarily need solutions today, but they could be something that is needed tomorrow.

Enhanced customer and stakeholder trust is another benefit and this in turn can help organizations open access to new markets, thereby giving them a competitive edge.

Greater operational resilience is an over-arching advantage of deploying solutions for digital sovereignty.



Organizations that use sensitive data for AI will find sovereign cloud of particular benefit. By using a sovereign cloud for non-anonymized data, they will not only increase their AI model’s performance but also eliminate any risks of exposing the workloads to non-European regulations.



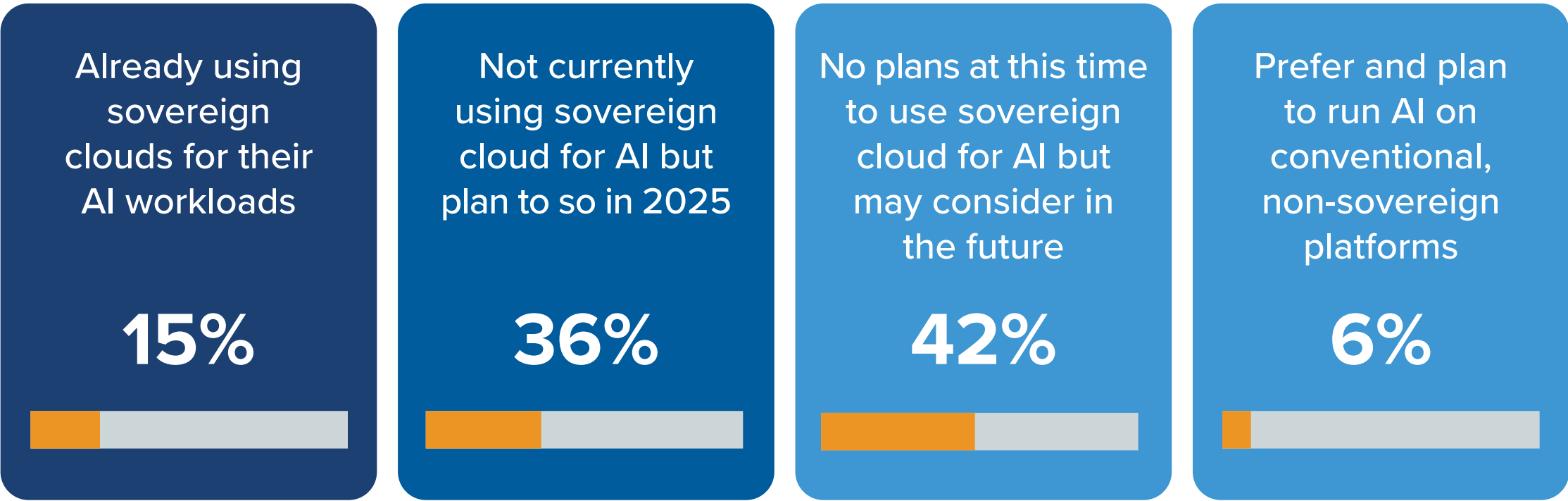
AI Workloads and Digital Sovereignty

AI adoption is accelerating, but organizations must ensure that critical AI workloads remain under their control. Digital sovereignty is not just about compliance — it is about ensuring security, resilience, and strategic autonomy while leveraging cloud AI capabilities.

Integration of AI with Sovereign Cloud

As AI becomes integral to business operations, ensuring that AI workloads align with digital sovereignty principles is crucial.

Organizations are increasingly recognizing the need to balance innovation with data governance and security.

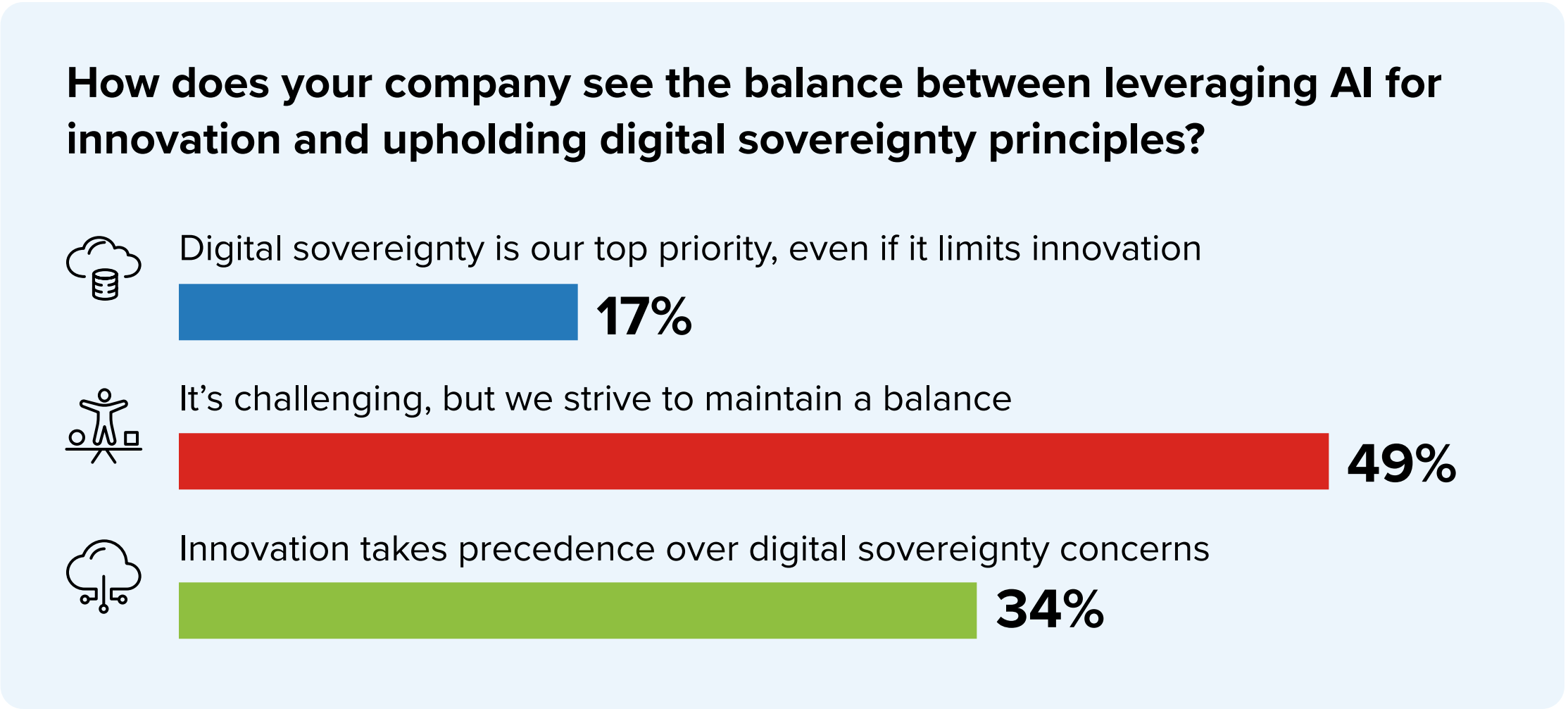


Current and Future Trends

Current Usage: Many companies currently prefer conventional, non-sovereign platforms for AI, with only 15% already using sovereign cloud for AI.

Future Plans: Interest to transition to sovereign clouds is growing, with 36% of European organizations planning to use sovereign cloud solutions by 2025.

Drivers and Challenges: This shift is driven by the need to comply with evolving regulations and to enhance data security and privacy, but half of companies are still challenged to find a balance between AI and sovereignty.



AI Workloads and Digital Sovereignty

Technology Partner Choices

Digital sovereignty is becoming a significant factor in selecting technology partners for AI projects.



Partner preferences:

Companies are looking for partners that offer local expertise and adhere to sovereign principles, ensuring both innovation and compliance.



Influence on choices:

44% of organizations consider digital sovereignty when choosing technology partners, 24% stress a preference for local providers.

How does the need for sovereignty solutions influence your company's technology partner choices for AI projects?

44%

We consider digital sovereignty as one of several factors when selecting technology partners.



32%

While we're aware of digital sovereignty, it does not significantly impact our partner choices.



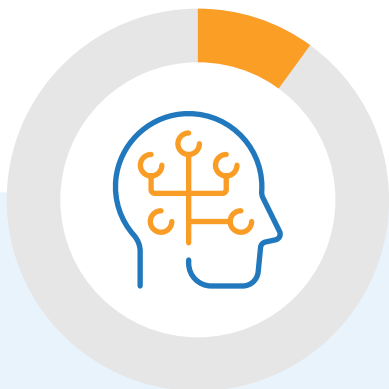
24%

It strongly influences our choices: We primarily partner with local technology providers.



10%

Our choices are based solely on the quality & effectiveness of the AI solutions partners offer.



Ensuring AI Sovereignty

Organizations prioritize different elements of AI platforms when ensuring sovereignty. Identifying the three most critical aspects helps shape strategies that align with regulatory, security, and operational needs.

Critical elements for AI sovereignty

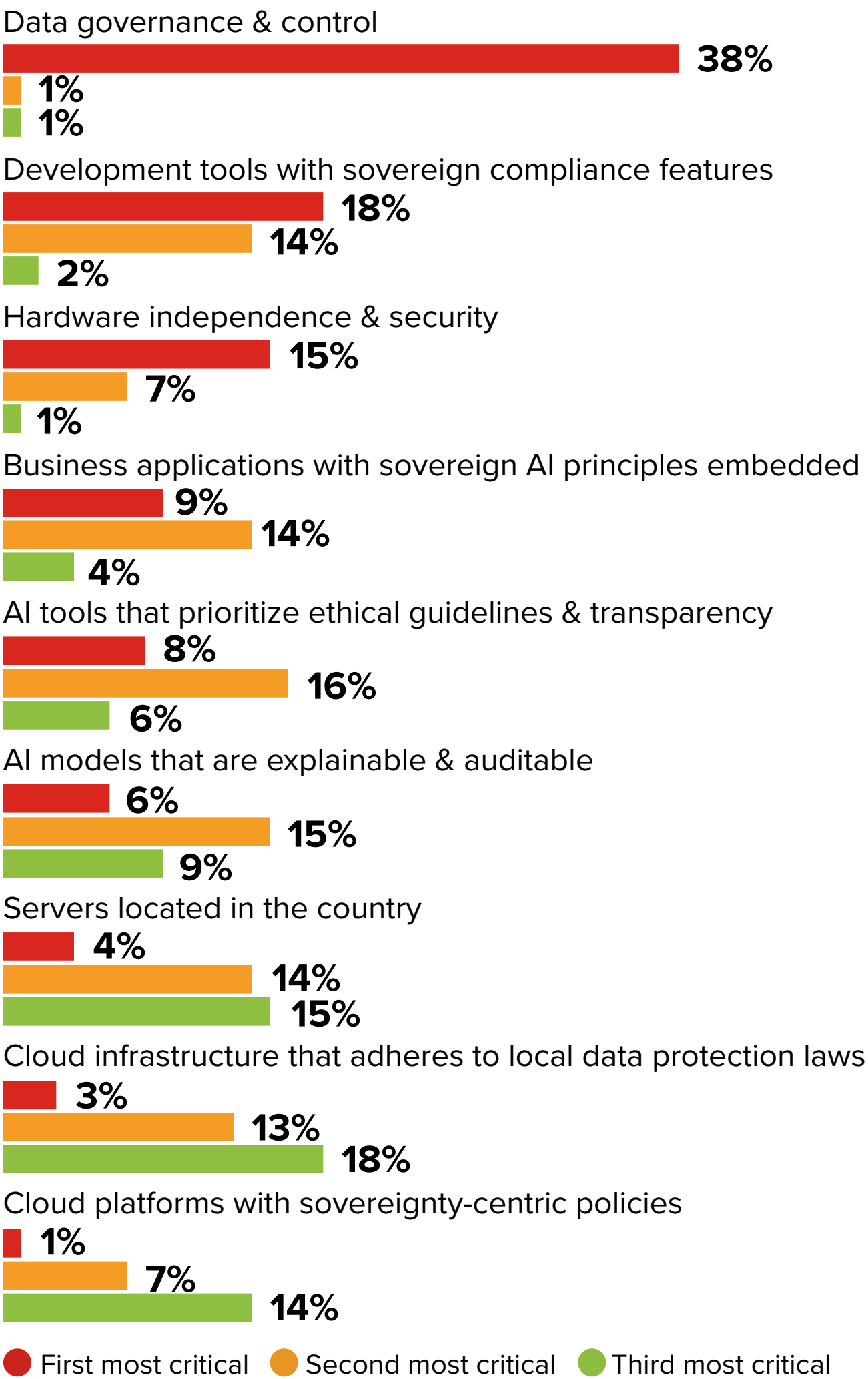
- Data Governance & Control: Ensuring that data used in AI models is managed and controlled in accordance with sovereign principles — an absolute must.
- AI Tools with Sovereign Compliance Feature: Using such AI tools facilitates AI development and takes some operational burden from an organization’s shoulders; strategic responsibility is still intact.
- Hardware Independence & Security: Utilizing secure and independent hardware to prevent unauthorized access and ensure data integrity.

Second tier but still crucial

- Cloud Infrastructure Compliance: Ensuring that cloud platforms adhere to local data protection laws and sovereignty-centric policies.
- AI Tools with Ethical Guidelines & Transparency: Implementing AI tools that prioritize ethical considerations and provide transparency in decision-making processes.
- Explainable AI Models: Developing AI models that are auditable and explainable, enhancing trust and accountability.
- Local Datacenters: Organizations consider ownership of in-country datacenters as a top attribute for sovereign cloud partners.
- Cloud infrastructure support for multitenancy along with security.

Partner perspective

- Organizations seek partners with expertise in data management, cybersecurity, and data classification to address skills gaps and support sovereign cloud strategies.
- Preference should be given to local partners who have a better understanding of the local market and culture and are bound by the same legal and regulatory obligations.
- Skills gaps need to be addressed. While 51% of organizations need help with data management and analytics, 50% require expertise in cybersecurity.



Master Challenges of Sovereign Cloud



Challenges

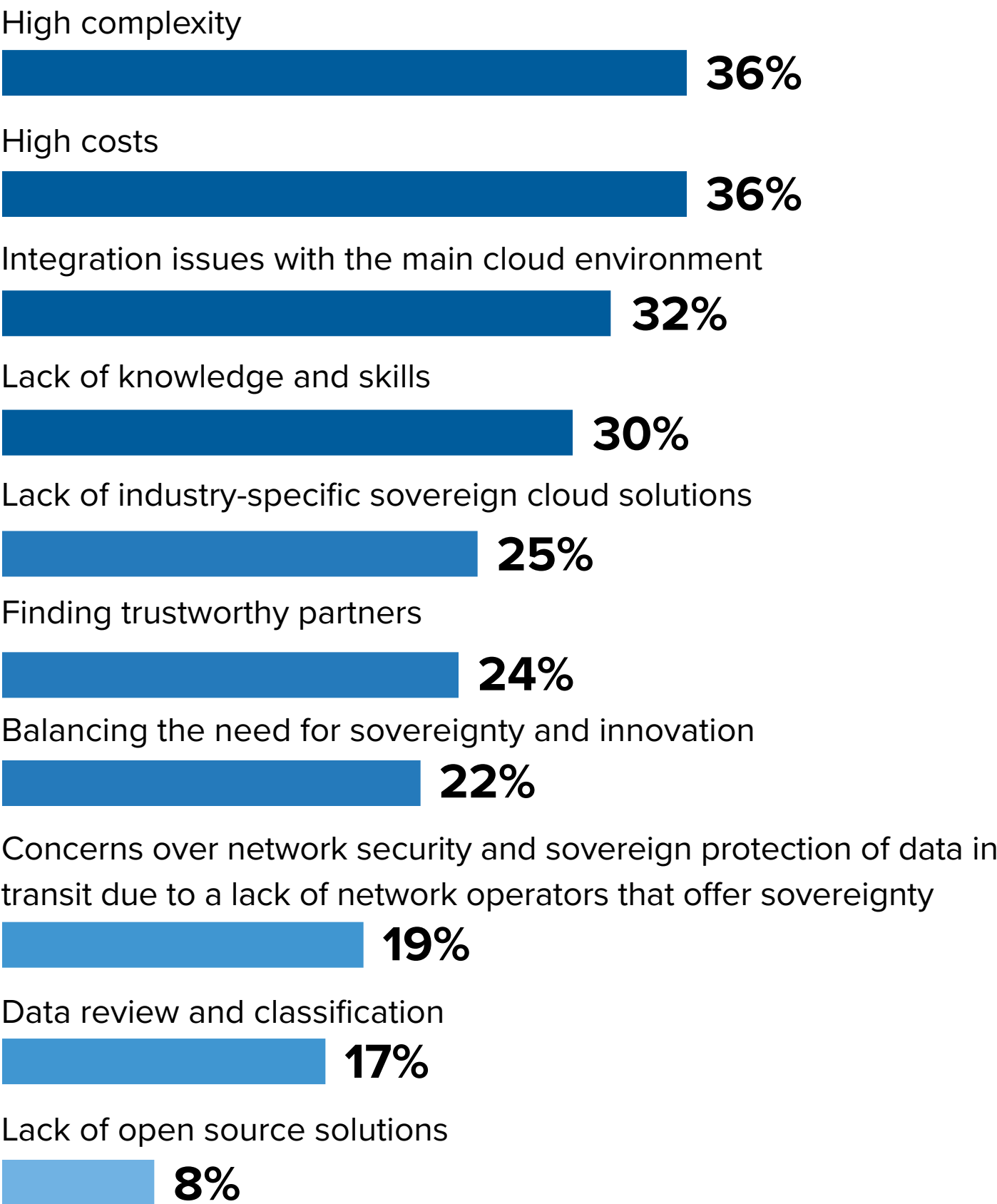
High complexity is one of the top challenges for organizations implementing solutions for digital sovereignty.

As well as the complexities of data classification, other difficulties include integrating a sovereign cloud into the main IT environment, ensuring solutions meet compliance and legal requirements over the long term, and selecting network partners who can assure the sovereignty of data in transit.

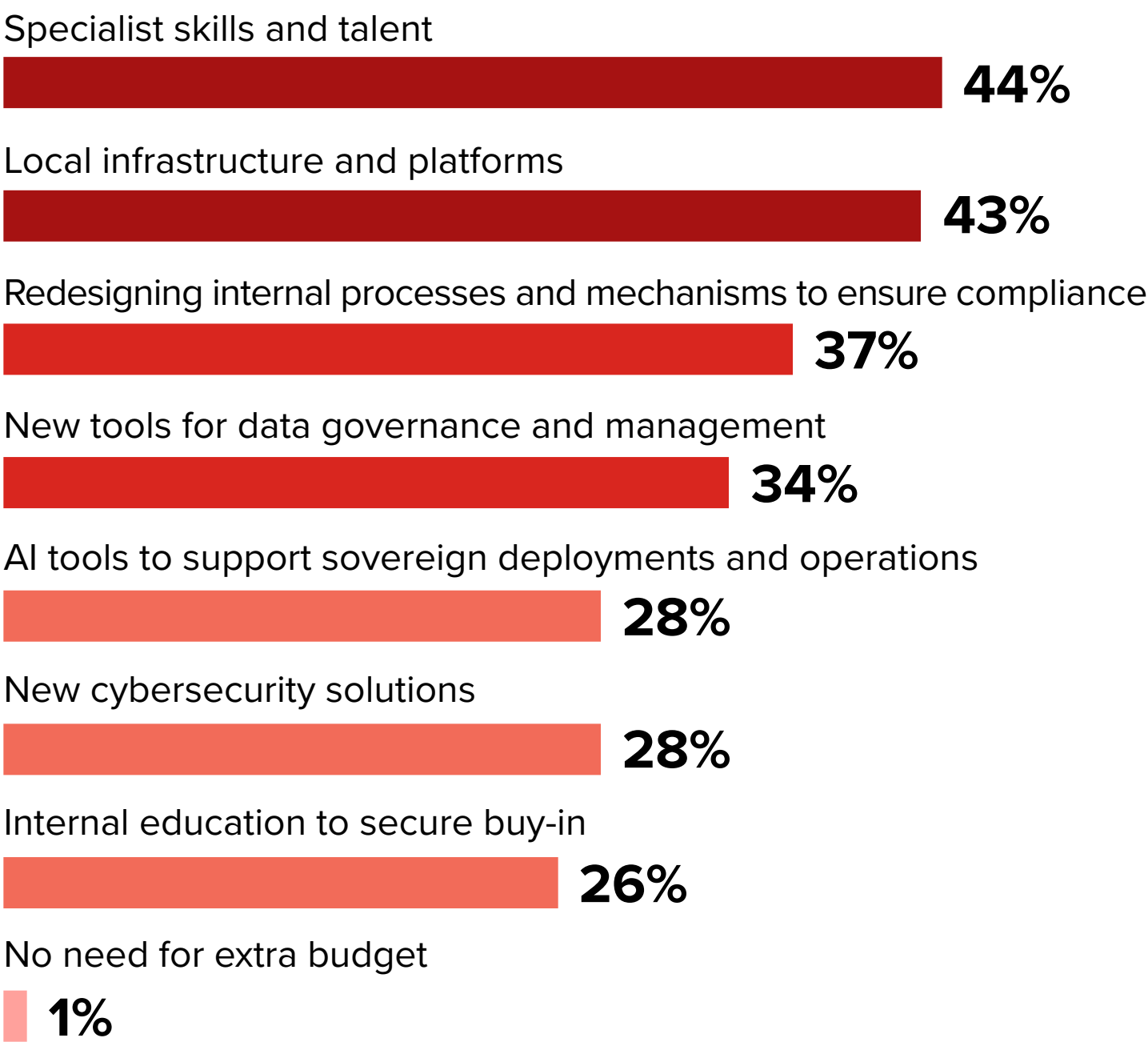
High costs are also regarded as a top challenge. Decision makers who use sovereign cloud will need to consider the additional investments that include new platforms and infrastructure, new tools for security and governance, and training and upskilling.

A lack of open-source solutions will become a bigger challenge once sovereign cloud usage begins to mature, especially to help avoid vendor lock-in. Using industry standards is also crucial here.

Customer pain points to address



Areas that will require extra budget for implementing sovereign solutions



Digital Sovereignty Success — Choosing Partners with Expertise

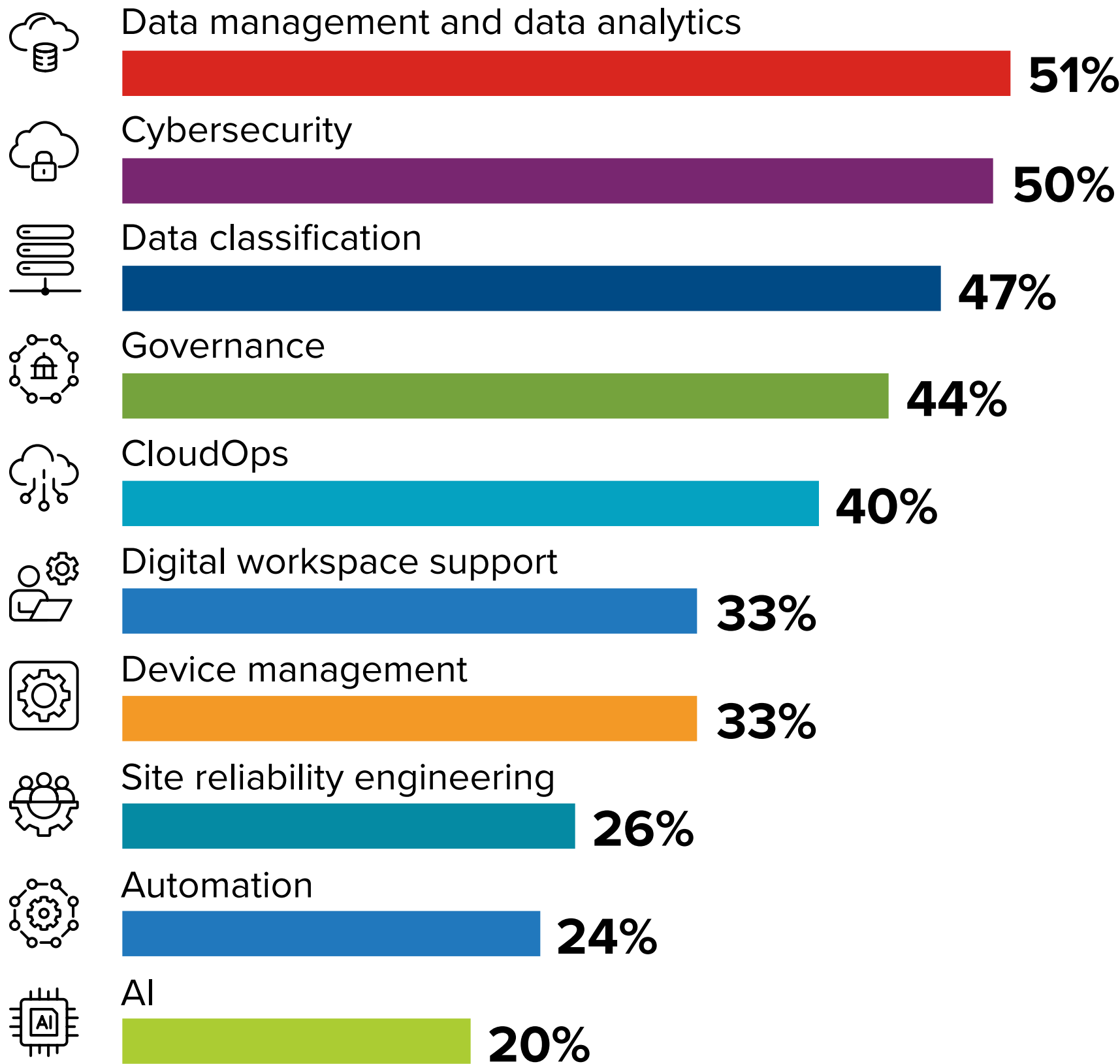


Organizations seeking sovereign cloud solutions will look for trusted partners who can help address all their challenges.



Generally speaking, organizations will also need partner support for assessing and defining the scope of a sovereign cloud strategy to help win additional budgets and corporate mindshare.

What additional skills and training are needed to address emerging digital sovereignty needs?



Digital Sovereignty Success — Choosing the Right Partner

When choosing a partner for digital sovereignty, organizations focus on trust, control, and alignment with local regulations.

They prioritize partners with local datacenter ownership, national certifications, and no vendor lock-in, reflecting a strong need to protect data from all unauthorized and extra-territorial access.

When looking for a partner, many organizations rely on network recommendations rather than vendor marketing, showing that peer trust is key, given the sensitive nature of digital sovereignty.

Organizations also involve partners early in the decision-making process, treating sovereignty as a strategic priority. Increasing demand for managed services alongside sovereign cloud solutions highlights the need for simplicity without compromising data control.



Which attributes do you consider important when choosing a sovereign cloud partner or provider?



Digital Sovereignty Success — Working Within Sovereign Ecosystems



A trusted ecosystem of partners is needed for sovereignty to work at scale.



For global cloud players, that means looking for the right regional and in-country partners to help boost local credibility and to deliver local services and local expertise and leverage local knowledge.



For the local service providers, it means partnering with global players to help deliver innovation and scalability — a sovereign cloud need not be a limited cloud!



The global SaaS providers then need to be able to work with both global and local partners to develop and deliver customized offerings within sovereign frameworks.



Vivicta is a company employing about 7,000 experts with revenue of around EUR 1 billion. Its offerings include digital transformation services, cloud, security and infrastructure solutions, data management, app development, and artificial intelligence.

Digital Sovereignty Offerings



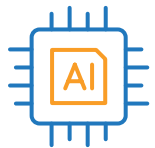
Strategic Approach

Vivicta is committed to meeting its customers’ evolving demands by providing multi-cloud solutions across hybrid, private and public environments. Its datacenters are strategically located throughout the Nordic countries, ensuring robust, sovereign digital infrastructure.



Operational and Technical Sovereignty

The company’s sovereignty approach addresses multiple dimensions featuring local datacenter solutions across Nordic countries, connected via Nordic network providers, giving customers confidence regarding data location, compliance requirements, and jurisdictional control. Vivicta maintains clear ownership and access controls, with specific named personnel managing customer environments. For **operational sovereignty**, they provide transparency in regard to environment management, primarily employing European-based staff through onshore and nearshore delivery models. This approach allows regulated sectors to maintain compliance while benefiting from cloud capabilities. Their **technical sovereignty** strategy includes hybrid and private cloud implementations built specifically to satisfy customers’ varying sovereignty requirements.



AI Sovereignty Solution

Vivicta’s AI sovereignty capabilities help customers achieve data sovereignty and unlock advanced AI use cases. The solution includes dedicated infrastructure, development tools, and AI frameworks. The AI sovereignty model empowers organizations to choose where and how their models process sensitive data, ensuring compliance with local regulations, security standards, and operational preferences. The principle of “bringing AI to your data” emphasizes control over data while harnessing AI’s power.



Digital Sovereignty Challenges & Client Needs

Vivicta’s clients have diverse sovereignty needs, driven by regulations, data sensitivity, and the desire for technical control. Key challenges include growing scrutiny over data ownership, changing data flows, and questions about jurisdiction.

The rise of AI has made data sovereignty even more critical, especially for handling confidential data. Meanwhile, geopolitical tensions are prompting organizations to rethink digital asset strategies and reassess vendor trust. Many clients seek AI sovereignty through a flexible hybrid approach that adapts to data sensitivity and long-term costs. Sovereign AI solutions also enhance data resiliency. This is especially urgent in highly regulated sectors, such as healthcare, where strict rules may block standard public cloud use for AI. The core challenge is balancing data-sharing benefits with strong, targeted security and control.



RedHat Partnership:

Red Hat technologies are an important part of Vivicta’s hybrid cloud strategy, ensuring consistency across a diverse range of environments. The partnership enables the seamless integration of cloud platforms under unified management. To achieve AI sovereignty, Vivicta uses Red Hat OpenShift to run its generative AI stack and OpenShift’s AI module for comprehensive workloads. Red Hat’s curated open-source technologies uphold sovereignty principles by providing cloud-native capabilities such as self-service provisioning, API-driven development and infrastructure as code. This partnership benefits customers by delivering a consistent experience regardless of deployment location, thereby enhancing flexibility and efficiency. The partnership excels in hybrid scenarios, enabling workloads to span various environments and ensuring robust performance and compliance with sovereignty requirements.

Recommendations for Clients



Choose Providers with Local Expertise:

Select technology partners with deep knowledge of local regulations, compliance requirements, and the cultural landscape. This ensures that your sovereignty needs are met while aligning with national data protection laws.



Focus on Flexibility and Avoid Vendor Lock-In:

Prioritize solutions that allow data interoperability and portability, such as open-source platforms. This helps prevent being locked into proprietary systems, ensuring future flexibility as your sovereignty needs evolve.



Invest in Training and Skills Development:

Given the complexity of digital sovereignty, make sure your teams are equipped with the necessary skills in areas like data management, cybersecurity, and compliance. Partner with experts to bridge any skills gaps and facilitate the smooth integration of sovereign solutions into your IT infrastructure.



Ensure Comprehensive Data Control and Security:

Look for solutions that give you full control over your data, both in transit and at rest. Ensure that your data is protected from external access and that providers offer robust security measures to safeguard critical information.



Seek Partners with Sovereignty-Compliant AI Solutions:

As AI becomes increasingly important, ensure that AI tools and workloads comply with digital sovereignty principles, including ethical guidelines, data governance, and security features.

About the Analysts



Ewa Zborowska,
Research Director,
AI, Europe

Ewa Zborowska is an experienced technology professional with 25 years of expertise in the European IT industry. Since 2003, she has been a member of the IDC team, based in Warsaw, researching IT services markets. In 2018, she joined the European team with a specific emphasis on cloud and AI. Ewa is currently the lead analyst for IDC’s European Artificial Intelligence Innovations and Strategies CIS.

[More about Ewa Zborowska](#)



Rahiel Nasir,
Research Director,
European Cloud Practice

Rahiel Nasir is responsible for leading and contributing to IDC’s European cloud and cloud data management research programs, as well as supporting associated consulting projects. In addition, he leads IDC’s worldwide Digital Sovereignty research program.

[More about Rahiel Nasir](#)

Message from the Sponsor



As digital sovereignty becomes a central focus for governments and organizations worldwide, Red Hat recognizes the importance of open, interoperable technologies in enabling greater control over data, infrastructure, and operations. Building on decades of leadership in open source and hybrid cloud innovation, Red Hat supports approaches that prioritize transparency, security, and regulatory alignment, critical elements for sovereign digital infrastructures. As demand for sovereign cloud solutions rises, particularly in the context of expanding AI adoption and evolving compliance requirements, organizations must navigate technical complexity and avoid vendor lock-in.

Red Hat is committed to supporting this journey with technologies that foster flexibility, resilience, and long-term adaptability in an open hybrid cloud environment.

Your journey to a successful digital sovereignty strategy starts here.

www.redhat.com/en/engage/hybrid-sovereign-cloud-in-emea



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.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC’s analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world’s leading tech media, data, and marketing services company.



This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC’s Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

© 2025 IDC Research, Inc. IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC’s endorsement of the sponsor’s or licensee’s products or strategies.



IDC UK
5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom
T 44.208.987.7100



© 2025 IDC Research, Inc. IDC materials are licensed [for external use](#), and in no way does the use or publication of IDC research indicate IDC’s endorsement of the sponsor’s or licensee’s products or strategies.

[Privacy Policy](#) | [CCPA](#)