IDC

SPOTLIGHT

Sponsored by: Wasabi

Data sovereignty is now a board-level strategic imperative, driven by geopolitical instability and IT dependency risks. The practical response is sovereign architecture: layered, portable, and resilience led.

Cloud Without Compromise: Building Data Sovereignty into Your Infrastructure with a Resilience-First and Risk-Mitigating Approach

May 2026

Written by: Archana Venkatraman, Senior Research Director, Cloud Data Management

Introduction

The operating environment facing EMEA organizations in 2026 is best described as brittle, anxious, uncertain, and nonlinear. Amid this, the broader imperative is digital sovereignty: the capacity of nations, organizations, and individuals to govern their data, infrastructure, and capabilities free from external override, as IDC defines it. EMEA organizations face a regulatory environment shifting faster than procurement cycles. Geopolitical turbulence, cascading regulations, rising AI stakes, and structural concentration in a handful of hyperscalers have exposed a fundamental vulnerability: organizations can rarely control the legal and regulatory landscape of any given country, but they can control where their data lives and how it is governed.

These dependencies carry systemic consequences and business continuity risks, moving sovereignty from a nice-to-have and a legal team's desire to a top-of-mind boardroom agenda. It is fast-evolving from a sentimental or protectionist hype to a strategic imperative. According to IDC research, data sovereignty now outranks growth and innovation as a strategic priority for one in every four organizations,.

AT A GLANCE

KEY STATS

By 2028, due to geopolitical uncertainties, 60% of organizations with digital sovereignty requirements will migrate sensitive workloads to new cloud environments to reduce risk and increase autonomy

WHAT'S IMPORTANT

A mature and intensified hybrid cloud and multicloud strategy is one that treats sovereignty as a layered operating model built on resilience, control, portability, and commercial optionality, rather than as a blunt, absolutist demand for data isolation with an on-premises only strategy

Addressing absolute digital sovereignty and control is a multi-year journey and an overwhelming and disruptive one at that. For most enterprises, getting data location right is the first viable starting point. Managing where data sits is a necessary condition for sovereignty. Its real leverage is that it makes all other layers possible, be it encryption, access governance, audit compliance, portability, and recovery independence because they all depend on having a controlled, documented data residency layer underneath them. It is the foundation of regulatory compliance. GDPR, the EU Data Act, NIS2, and most national frameworks are fundamentally about where data is processed and stored and whose laws govern it. It also directly enables audit trails, documented access controls, and the kind of provenance reporting that regulators increasingly require.

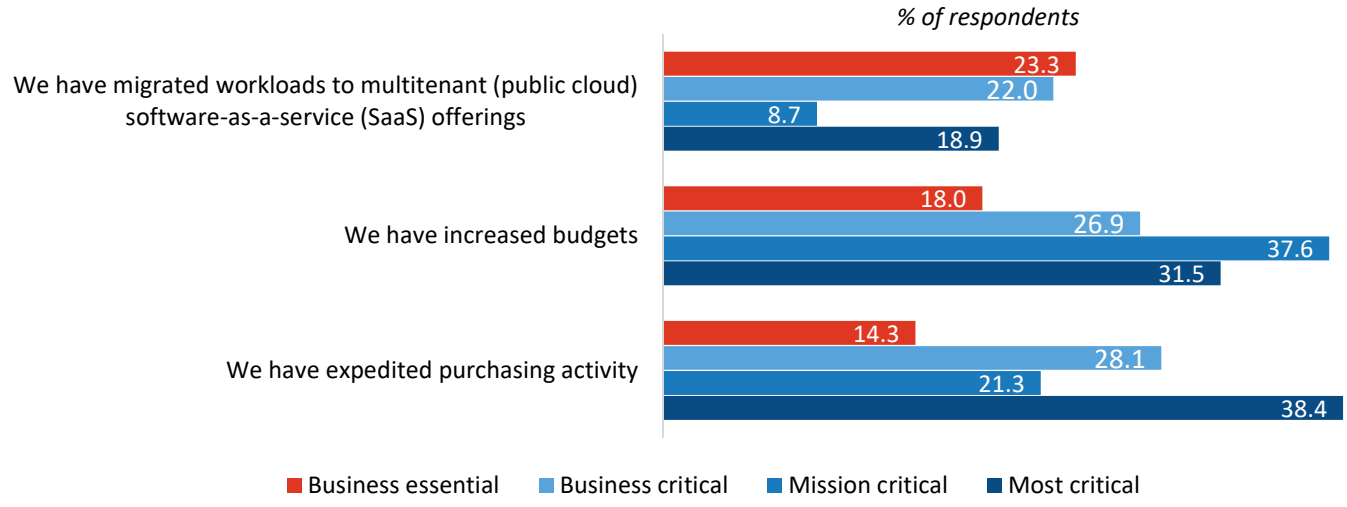
IDC believes that data locality, the ability to determine where data physically resides, is the most actionable dimension of sovereignty and the one organizations can most directly control. Many view this as a core pillar of enterprise risk management and competitive strategy. As geopolitical uncertainties continue to intensify, organizations are increasingly acting on these priorities: according to IDC FutureScape: Worldwide Cloud 2026 Predictions (IDC #US53859425, October 2025), by 2028, 60% of organizations with digital sovereignty requirements will migrate sensitive workloads to new cloud environments to reduce risk and increase autonomy.

EMEA organizations have already started laying the groundwork. According to IDC's December 2025 *CloudOps and Governance Survey*, 69% of organizations are increasing their data governance, sovereignty, security, and resilience budgets for 2026. There is no mass exit or cloud U-turn. In fact, only 23% of organizations admit to repatriating data from the cloud. A higher number of organizations have taken other steps, such as completing data inventory and classification exercises; creating budgets and teams for sovereignty, risk, and resilience management; and better understanding cloud shared responsibilities. As illustrated in Figure 1, when it comes to the most critical workloads, 38% of organizations have expedited infrastructure purchasing activities to mitigate risks and 32% have increased budgets. In comparison, for business-essential workloads, a higher number of organizations are adopting multitenant environments.

This represents a mature and intensified hybrid cloud and multicloud strategy: one that treats sovereignty as a layered operating model built on resilience, control, portability, and commercial optionality, rather than as a blunt, absolutist demand for data isolation with an on-premises strategy that is likely to reintroduce problems such as lack of scale and speed, high CapEx investments, and limited access to cloud innovation.

EMEA organizations are moving away from theoretical purity on sovereignty and toward architecture-led pragmatism. That means treating data sovereignty not as a destination but as an ongoing discipline to be designed into their infrastructure.

FIGURE 1: ***EMEA organizations' response to business risks for each workload category***



n = 509

Source: IDC's CloudOps and Governance Survey, December 2025

In summary, IDC believes EMEA organizations are moving away from theoretical purity on sovereignty and toward architecture-led pragmatism. That means treating data sovereignty not as a destination but as an ongoing discipline to be designed into their infrastructure. The goal is to reduce exposure while preserving innovation, flexibility, and speed. Cloud storage, leveraged as an independent, sovereign-ready layer, plays a central role in making this possible.

Definitions

Sovereignty risks becoming too abstract and inactionable without rooting it in the business outcomes of trust, resilience, innovation, and control. Digital sovereignty is multilayered. It encompasses the ability of an organization or nation to govern its own digital assets, infrastructure, and capabilities free from external override. Within this, data sovereignty is the fundamental starting point: the ability to govern where data resides, which laws apply to it, who can access it, and how it can be protected and recovered. Other dimensions, whether AI sovereignty, skills sovereignty, or operational sovereignty, depend on getting data sovereignty right.

The core dimensions of meeting the principles of data sovereignty are framed in Table 1. Taken together, they form a practical operating framework that organizations can use to assess their current posture and prioritize investment.

TABLE 1: ***The four dimensions of data sovereignty: Definitions, requirements, and cloud feature sets***

DIMENSIONS	DEFINITIONS	KEY REQUIREMENTS	CLOUD FEATURES TO LOOK FOR
Data	Governs where data physically resides and who can access it	Residency, encryption, access control	Regional data center choice across EU/EMEA; customer-managed encryption keys; replication; granular access policies.
Legal	Determines which legal jurisdiction governs data and who holds override powers	Jurisdiction clarity, contract terms, subpoena risk	Customer choice on where data is stored
Operational	Ensures continuity and recovery even if a primary provider is disrupted	Security, data resilience, flexibility and industry standards	Immutable and invisible object storage; WORM compliance; replication; seamless backup/recovery integration
Technical	Preserves the ability to move, recover, and exit without vendor dependency	Immutability, data portability or exit readiness	S3-compatible API for multicloud portability; no egress fees; scalability and flexibility across hybrid architectures; contractual transparency on data migration

Source: IDC, 2026

Sovereignty is not a product category. It is the outcome of governance, architecture, and operating decisions. No single vendor delivers end-to-end sovereignty. But each layer of the technology stack, starting with data storage, acts as either a constraint or an enabler for the layers above. The three questions that executives should be able to answer are:

- Can you control your sensitive data? (Do you have flexibility and choice of locations, data visibility, and portability?)
- Can you manage, secure, and govern the data independently? (Do you have control of security, policies, data residency, and encryption?)
- Can you move the data if conditions change? (Is the environment interoperable, portable, and transparent?)

Benefits

When executed well, data sovereignty goes beyond mundane compliance to a trusted, robust, and resilient data architecture. IDC urges organizations to shift the framing from fear-based compliance toward strategic advantage. A resilience- and autonomy-led approach to sovereignty delivers meaningful benefits across the following five dimensions:

- **Reduced geopolitical and jurisdictional exposure:** Organizations that can demonstrate clear data residency are better positioned to document and potentially enforce data location requirements, which constitutes a meaningful risk mitigation lever in sovereignty discussions. While data location alone does not neutralize jurisdictional risk or cross-border enforcement, it provides a documented, auditable foundation. As the regulatory environment in EMEA continues to evolve, with GDPR, NIS2, the EU Data Act, and a growing body of national frameworks placing new obligations on data management, demonstrating where data resides and how it is governed is a baseline expectation.
- **Higher resilience and continuity:** A sovereignty-led architecture is, by design, a more resilient one. Organizations that distribute data storage across independent providers, rather than concentrating the storage within a single hyperscale environment, reduce the blast radius of any single point of failure. Immutable, geographically distributed storage is a business continuity imperative.
- **Greater operational control:** Independent data storage and governance layers give organizations meaningful control over access policies, encryption key management, and data life-cycle decisions. This operational control is especially valuable in sectors where regulatory mandates require documented audit trails, retention schedules, and the ability to demonstrate that data has not been accessed or modified without authorization.
- **Commercial resilience:** Vendor concentration is a commercial risk. Organizations that have built their data estates around a single hyperscale provider face asymmetric negotiating dynamics: high egress costs, restrictive contractual terms, and limited leverage when pricing changes or service disruptions occur. Sovereign architecture — characterized by portability, interoperability, and independent storage layers — restores commercial balance and protects organizations from lock-in at a time when cloud pricing and policy are increasingly contested terrain.
- **More headroom for innovation:** Paradoxically, a strong sovereignty posture creates more room for innovation, not less. Confidence in data is the precondition for confident AI adoption, data product development, and cross-border data collaboration. Organizations that trust their data control and resilience posture can shift resources from reactive firefighting to innovation and competitive differentiation.

Trends

Digital sovereignty has crossed into the mainstream of enterprise IT strategy, driven by a combination of regulatory pressure, geopolitical instability, and dependency risks caused by single-cloud concentration. IDC predicts that by 2028, CIOs at multinationals will boost investments in modular, sovereign-ready cloud and data localization environments by 65% to future proof operations against rising sovereignty demands.

For multinationals operating across EMEA, the risk calculus has shifted materially: the possibility of sudden regulatory changes, sanctions, or access restrictions is no longer theoretical given the current geopolitical developments.

Yet despite this urgency, there remains limited clarity in the market about what sovereignty demands in digital operations. Organizations are developing a spectrum of responses, ranging from pragmatic architectural decisions to overcorrections that confuse location-only controls with full digital sovereignty. Therefore, clarity on what sovereignty is, and importantly, what it shouldn't become is critical.

What sovereignty is NOT

IDC observes that the EMEA market is not moving toward cloud repatriation in response to data sovereignty.

In competitive sectors such as U.K. banking and financial services, a laser focus on AI-driven innovation combined with existing mature risk management and compliance approaches is guiding organizations to take a risk-based and practical approach to sovereignty.

Wholesale migration back to on-premises infrastructure would sacrifice the agility, economics, and scalability that modern organizations require. Instead, what IDC observes is a market moving toward sovereign architecture patterns, layered onto hybrid cloud, multicloud, and distributed storage estates for flexibility, interoperability, and location choice without abandoning cloud economics.

According to IDC's March 2026 *FERS Survey* that assesses the impact of the Middle East War on IT trends, 35% of digital-native organizations are prioritizing cloud and datacenter resilience through multi–availability zone and multiregion investments in the next 6–12 months, with only 18% investing in sovereign or locally owned datacenters. This further validates that mass repatriation is not seen as a practical answer to rising sovereignty concerns.

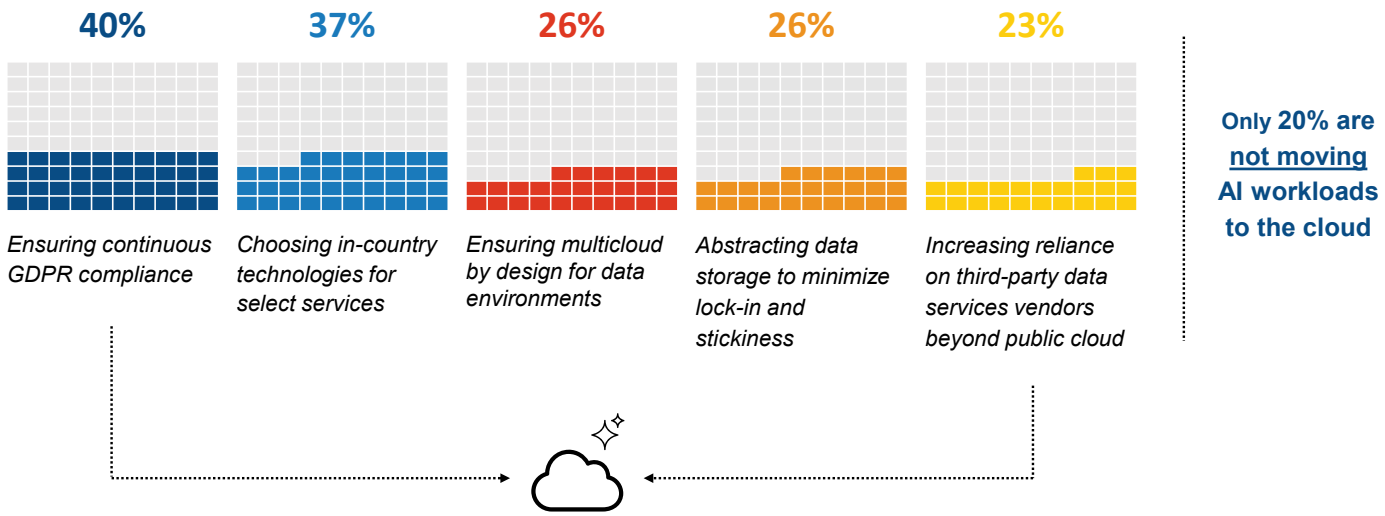
In addition, 44% of digital natives identified "supplier diversification" as an IT architecture sourcing strategy amid the Middle East War compared with 20% choosing local sovereign datacenters.

There is also a notable divergence between digital natives and digital followers. Digital-native organizations tend to approach sovereignty pragmatically, focusing on resilience and operational autonomy. A higher proportion of digital followers are drawn to location-only, EU vendor–only policies without proportionate risk reduction. IDC's view is that the next phase of sovereignty in EMEA will be won through design choices that preserve optionality, not through either/or restrictions.

In IDC's opinion, IT teams are under pressure to ensure resilience within stipulated budgets, making cloud economics still very attractive for storage and archiving purposes.

Following data classifications, organizations are taking a nuanced risk-mitigation approach, implementing appropriate technical measures depending on the risk exposures, as shown in Figure 2.

FIGURE 2: ***Technical mechanisms to address data sovereignty concerns***



n = 509

Source: IDC's CloudOps and Governance Survey, December 2025

Portability is becoming a design principle

By 2027, 70% of the G5000 will reengineer most core workloads to be portable across private and public cloud environments in response to resilience, AI, and privacy regulations. Organizations are increasingly evaluating cloud storage and infrastructure partners not just on current capability but on their ability to support exit readiness and cross-environment mobility. Portability is not a new concept and is an architectural aspiration but a difficult operational reality. Workloads with significant data gravity, tightly coupled to proprietary hyperscale APIs, have historically made workload migration costly and disruptive. The key enablers are standardized object storage APIs (particularly S3-compatible interfaces), modern backup and data management architectures that decouple data from compute, and a deliberate architectural shift toward treating storage as an independent, substitutable layer.

Ultimately, such architectural flexibility gives organizations greater control over where data resides, how it moves, and which jurisdictions and providers govern access to it, thereby strengthening data locality and digital sovereignty strategies.

Metadata control is gaining strategic importance

Control of metadata, copy data, and archive data placement is becoming a critical dimension of business continuity strategy. As regulatory requirements around data retention, audit trails, and recovery expand, the ability to manage the full data life cycle, including secondary copies and long-term archives, in a compatible but different storage environment is essential.

Considering Wasabi

The argument for placing storage at the center of any practical sovereignty strategy is straightforward: storage is where control, retention, immutability, and recoverability become real. Abstract sovereignty commitments mean nothing if the underlying data can be accessed, modified, moved, or locked by a third party outside the organization's governance framework. Selecting an independent object storage layer – that help IT teams address the four dimensions of data sovereignty - is one of the most high-impact architectural decisions an EMEA organization can make.

Why storage is central to practical sovereignty

An independent storage tier that is architecturally decoupled from the primary compute environment creates a meaningful sovereignty buffer without sacrificing cloud economics or operational agility. Hyperscale cloud providers offer compelling economics and capabilities, but they also introduce concentration risk. When storage, compute, network, and application services are sourced from a single provider, the organization's sovereignty posture is constrained by that provider's jurisdictional exposure, contractual terms, and business continuity commitments.

How Wasabi addresses EMEA sovereignty requirements

Wasabi is an independent cloud object storage provider that positions itself as a high-performance, cost-efficient alternative to hyperscale storage services. In the context of EMEA data sovereignty, Wasabi's architecture and commercial model align with several of the practical sovereignty requirements identified in this paper, including:

- **Regional deployment choice:** Wasabi operates storage regions across EMEA, including locations in Amsterdam, Frankfurt, London, Paris, and Milan. This enables organizations to enforce data residency requirements without sacrificing cloud-native storage capabilities.
- **Independent object storage layer:** Wasabi's S3-compatible API allows organizations to integrate the company's storage into existing workflows, backup solutions, and multicloud architectures without creating new dependencies on a single provider. This is the practical foundation of the portability-by-design principle.
- **Immutable and invisible storage:** Wasabi supports WORM (write once, read many) object storage for regulatory compliance and ransomware resilience. Its Covert Copy capability, a new innovation that enables hidden, tamper-resistant secondary copies of critical data, extends this protection, ensuring that backup data remains accessible for recovery even if primary copies are compromised or deleted.
- **Hybrid cloud and multicloud compatibility:** Wasabi integrates natively with leading backup, recovery, and data management platforms, enabling organizations to build sovereign storage layers into hybrid cloud and multicloud architectures without costly reengineering.

Connecting Wasabi to the sovereignty framework

When mapped against the four-lens sovereignty framework introduced in Table 1, Wasabi offers:

- **Data control:** Wasabi helps enforce policies around where data is stored, with regional choice and role-based access controls and policy-driven access management.
- **Operational autonomy:** Wasabi provides a governance layer for backup, recovery, and data life-cycle management that is independent of primary hyperscale environments.

- **Technical resilience:** Immutability, Covert Copy, multi-user authorization, and WORM capabilities protect against ransomware, accidental deletion, and malicious interference.
- **Strategic autonomy:** Wasabi's S3-compatible, no-egress-fee model supports scalability, flexibility, and exit readiness, reducing lock-in and preserving commercial negotiating leverage across environments.

Challenges and executive considerations

No single provider delivers end-to-end sovereignty. Storage is one of the most important practical levers for achieving sovereignty outcomes, but it is not sufficient on its own. Outcomes depend equally on data classification, encryption and key management strategy, policy design, risk governance, and the broader architectural decisions made across the data estate. Wasabi should be evaluated as a component of a sovereign architecture, not as a turnkey sovereignty solution.

Wasabi is also a United States–headquartered company. This is a material consideration for some EMEA buyers, particularly in the public sector and in jurisdictions where procurement frameworks increasingly require EU-registered vendors, local billing entities, or country-specific support arrangements. While Wasabi operates datacenters within the EU and stores data under applicable local law, IDC recommends buyers with the strictest sovereignty requirements, including requirements for EU corporate registration or national-level provenance, should conduct detailed due diligence to assess whether Wasabi's current operating structure meets their specific obligations. IDC recommends that organizations evaluate this dimension explicitly as part of their vendor assessment, rather than assuming that geographic data location is sufficient to satisfy all sovereignty requirements.

That said, in conversations with IDC, savvy organizations that balance innovation, resilience, and sovereignty are adopting the following strategies to win all stakeholders:

- **Reframing the question:** Corporate domicile and operational data control are different things; only the latter materially affects sovereignty posture.
- **Defusing the CLOUD Act:** While the risk is real, savvy organizations understand that this risk may be overstated and that customer-managed encryption keys are a strong way to mitigate challenges.
- **Validating the EU providers:** Exploring whether some EU-registered vendors subprocess through U.S. entities is important, as a corporate wrapper is not equal to absolute sovereignty; a complete bill of materials analysis could identify supply chain risks, making it impossible to mitigate all risks.
- **Understanding the sector needs:** Not all enterprises require the due diligence for every data and workload like defense, intelligence, and CNI buyers — which have hard regulatory mandates — do.
- **Broad compliance:** Savvy organizations conduct due diligence on the basics, such as whether the diversified cloud vendors support regulations such as GDPR and have certifications and controls including SOC 2 and ISO 27001 for their datacenter deployments and storage environment.

Wasabi has demonstrated empathy and responsiveness to EMEA sovereignty desires. Wasabi's strong EMEA executive leadership team influences the engineering roadmap, the company is working with its channel partners to address sovereign data requirements across EMEA, and it is actively investing in datacenters across Europe (Amsterdam, Paris, Frankfurt, Milan, and the United Kingdom), as well as in engineering capabilities to give more data control and security capabilities to its customers.

Cloud vendors need to continue to expand EMEA regional footprints, strengthen data governance capabilities, and address the provenance concerns of the most sovereignty-sensitive buyers; companies have a significant and growing market opportunity. They should also consider a "better together" strategy with a data protection provider to cover all bases of sovereign data services. Last, companies should highlight compliance with data regulations in EMEA as well as security certifications.

Amid tremendous sovereignty-washing in the industry, cloud vendors should avoid over-rotating on the theme and focus on other strong business outcomes they deliver such as ease of use, strong cloud economics, and customer-friendliness. Amid tremendous sovereignty-washing in the industry, Wasabi should avoid over-rotating on the theme and focus on other strong business outcomes it delivers such as ease of use, strong cloud economics, and customer-friendliness.

Conclusion

EMEA organizations that approach sovereignty as a checkbox compliance activity will find themselves repeatedly caught off guard. Those that treat it as a foundational design principle will build the trust, resilience, and operational control that a data-driven enterprise requires.

The urgency of mitigating data control risks is amplified by the rise of AI. Without appropriate data residency, governance, and recoverability, organizations lack the foundation for responsible AI.

The path forward is not to pursue theoretical purity or adopting only in-country IT vendors. It is to make a series of small, decisive operational choices, about where data is stored and how it is governed, how it is recovered, and how portable it is, that collectively build a sovereignty posture that is resilient, pragmatic, and commercially sustainable.

IDC recommendations for EMEA C-suite leaders

- **Shift the sovereignty lens:** Treat data sovereignty as a resilience mechanism that minimizes disruption and builds confidence for data-led innovation, not merely a compliance obligation.
- **Avoid the temptation of restricting to EU-based providers only:** Global cloud vendors and storage providers are reputed and established and have long-term global ambitions. They are also appreciative of nuanced regional needs and are building mechanisms to help their regional customers adhere to sovereignty principles. Risk analysis of how overstated the triggering of CLOUD Act is or what proportion of IT assets is truly at risk can help reframe the sovereignty argument in practical business terms and provide clarity to balance innovation and resilience.
- **Classify data and apply differentiated controls:** Not all data requires the same treatment. Identify sensitive, regulated, and mission-critical data sets and apply layered controls accordingly.
- **Build independent recovery and operational resilience:** Ensure backup and recovery architectures are decoupled from primary cloud providers. Immutable, offsite object storage is a critical safeguard.
- **Preserve portability and negotiating leverage:** Avoid deep vendor lock-in. Architect for exit readiness and interoperability across your hybrid cloud and multicloud estate.
- **Loop in multiple stakeholders:** Sovereignty spans legal, IT, security, compliance, and the business. Governance frameworks must reflect that breadth.

» **Align data sovereignty to AI resilience:** As AI workloads proliferate, sovereign data infrastructure becomes the foundation for compliant, trustworthy AI.

About the analyst

Archana Venkatraman, *Senior Research Director, Cloud Data Management*

Archana Venkatraman leads IDC's European CloudOps and Governance research as well as Cloud Data Management research. As part of the CloudOps focus, Archana analyzes multicloud management and operations, cloud economics and FinOps, observability, cloud consolidation, and cloud governance and control. A big focus of her research is on cloud value realization, cloud-native success, and operational excellence.

MESSAGE FROM THE SPONSOR

Through its commitment to transparency, accountability, and cyber resilience, Wasabi enables organizations to securely store, govern, and recover critical data while simplifying compliance and reducing operational risk.

Built on a defense-in-depth security model, Wasabi protects customer data through encryption at rest and in transit, MFA and SSO-enabled access controls, immutable Object Lock storage, and Covert Copy® virtual air-gapping technology for enhanced ransomware resilience. Furthermore, Wasabi infrastructure is hosted in secure, redundant data centers certified for SOC 2, ISO 27001, and PCI-DSS.

Wasabi supports major regulatory and industry frameworks including HIPAA, GDPR, CJIS, FERPA, SEC/FINRA, and CFTC requirements.

To learn more, visit the Wasabi Trust Center

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com