Spotlight, sponsored by:
Mitel

Extending Data Sovereignty to Unified Communications

WRITTEN BY:
Archana Venkatraman
Senior Research Director, IDC

PUBLISHED:
October 2026

Regulation, geopolitics, and AI are pushing sovereignty beyond storage and cloud infrastructure into calls, chat, and meetings. This IDC Spotlight explains why communications and collaboration data carry the same risk, and what a sovereignty-ready architecture should provide.

The report draws on IDC tech buyer surveys covering more than 3,000 technology decision-makers, including IDC's *CloudOps and Governance Survey*, the *Future Enterprise Resiliency and Spending Survey* (Waves 2, 3, and 4; 2026), and the 2025 *Multicloud Survey*.

Introduction

Sovereignty requirements are gathering momentum, as organizations want the ability to own their digital and data assets, infrastructure, and capabilities free of external override. As communications and collaboration data carry the same risks as storage and infrastructure in terms of data control, resilience, and continuity, it is important to extend sovereignty principles to all data-critical workloads, including unified communications.

At a glance

Key stats

- 69% of organizations are increasing budgets for data governance, sovereignty, security, and resilience in 2026.
- 40% of organizations prioritize SaaS application sovereignty, the category covering most communications and collaboration tools.
- 48% name IT leaders and the CTO as the stakeholders most concerned about data sovereignty, ahead of legal, risk, and compliance teams at 27%.

Sovereignty goes from compliance checkbox to boardroom mandate

Geopolitical shocks, tightening regulations, and economic uncertainty are pushing data sovereignty out of the legal department and into mainstream enterprise risk and technology strategy.

Geopolitical impacts on prices, profits, and business operations remain the top-ranked technology-related risk for multinational organizations in 2026, cited by 50% of respondents in IDC's *Future Enterprise Resiliency and Spending Survey* (July 2026), ahead of tariff-driven cost pressure and hardware supply constraints.

One in every four organizations today ranks data sovereignty as its highest priority, yet only 23% of organizations report repatriating data from the cloud, a sign that balancing sovereignty with innovation, not retreating from the cloud, is the preferred strategy.

By 2028, IDC expects CIOs at multinationals to boost investment in modular, sovereign-ready cloud and data localization environments by 65% to future-proof operations against rising sovereignty demands.

Calls, meetings, chat, and presence and directory data (plus the transcripts and summaries AI now generates from them) are personal, regulated, and constantly on the move across borders — exactly the profile for which sovereignty rules are written. Regulators are already naming communications platforms directly: France's 2026 public sector prohibition on Zoom, Microsoft Teams, and others extends sovereignty scrutiny beyond data residency and into the communications solution itself. Sovereignty-minded public sector buyers are extending the same scrutiny to productivity software once treated as out of scope, including word processors and spreadsheets.

Definitions

IDC defines digital sovereignty as the capacity to govern data, infrastructure, and capabilities free of external override. IDC treats sovereignty as four connected dimensions, with no single switch to flip:

- **Data control:** The ability to choose and prove where sensitive data resides, and who can see it
- **Operational autonomy:** The ability to manage, secure, and govern that data independently of any single provider
- **Technical resilience:** The ability to continue operations if a provider, region, or connection is disrupted
- **Strategic autonomy:** The ability to move data and workloads if conditions, providers, or regulations change

While these four dimensions were developed primarily for cloud infrastructure and storage, nothing about the definition limits them to storage. Every dimension applies just as directly to unified communications solutions.

Benefits

With the status quo approach to unified communications architecture, when calls, messages, and meetings originate inside a shared global cloud, four properties become harder for the customer to guarantee on their own terms, which sovereignty-oriented solutions are designed to restore:

1. Sovereignty becomes contractual rather than architectural, since data residency depends on the provider's routing and region policy instead of a structural fact.
2. Auditability depends on the vendor, as data lineage is reconstructed from provider-supplied logs on the provider's own retention schedule.
3. Optionality narrows, because architectural change follows the provider's road map and exit paths run through vendor-defined migration.
4. Resilience concentrates, as availability is bounded by the provider's centralized core; therefore, a regional outage can remove local calling with no independent fallback.

Regional datacenters and customer-managed encryption keys reduce exposure on some of these points, but do not remove the underlying dependency on a provider's cloud for the communications data to exist at all.

An alternative pattern is emerging in the market: A select few vendors that understand global customers' rising sovereignty concerns are treating private infrastructure as core architecture rather than legacy technology and ensuring innovation on private offerings is a top engineering priority. Therefore, choosing these private offerings no longer means settling for less. This helps technology buyers to break free from the either-or dilemma when it comes to innovation and resilience.

Three sovereignty-focused outcomes organizations seek today are reducing hyperscale dependency, improving recovery and resilience options, and preserving commercial flexibility. A communications platform decision that only loops in legal and procurement is out of step with who owns sovereignty concerns within the business.

IDC observes three broad patterns in the market:

- Multitenant cloud platforms that offer regional data residency, where signaling, presence, and analytics still traverse the provider's centralized control plane
- Cloud UC platforms extended with an on-premises gateway, where the on-premises component is typically limited to a network access point (e.g., a PSTN breakout), with no functional share of UC services
- Distributed architectures in which UC functionality itself, not just a gateway, resides in customer infrastructure, leaving the customer (instead of the cloud provider) with the final say over where data and control sit. Buyers should ask which pattern a given claim addresses before taking it at face value.

The hallmarks of sovereignty-minded design for unified communications platforms include the following:

- Encryption keys that already sit with the customer
- Operational autonomy in practice, with core telephony continuing to work independently of a single provider, whether the disruption is a lost cloud connection, a regional disruption, or a geopolitical event
- A partner and marketplace ecosystem that avoids vendor lock-in
- Transparent software bills of materials, and cyber-resilience and security certifications appropriate for global organizations

Together, these design choices are intended to enable organizations to advance their AI, innovation, and modernization strategies without having to trade away control, business continuity, or autonomy.

Buyers are not choosing between sovereign and global cloud. Most are building toward a blend, and the ability to move across that spectrum matters more than any single deployment model.

In IDC's 2025 Multicloud Survey, nine in ten organizations said they are doubling down on hybrid strategies for sovereignty-related reasons:

- Among organizations whose interest in sovereignty has increased, 39% plan to use a hybrid mix of local and global cloud (the single most popular response).
- Overall, 22% already use sovereign public cloud solutions today, and a further 37% plan to do so within 12 months.

In communications specifically, deployment flexibility across on-premises, private cloud, public cloud, and hybrid, chosen workload by workload rather than platform by platform, allows organizations with very different needs (e.g., a retail outlet, a hospital, and a government site) to meet those needs from the same underlying software.

Getting data out of a platform is rarely the hard part. Getting it into a different one and keeping AI under the same rules as everything else is the next testing ground for sovereignty.

Only 22% of survey respondents reported ensuring data portability by design as part of their sovereignty response, even though exporting chat history or call records from one platform rarely means it can be reimported cleanly into another.

AI workload sovereignty is already a top 3 priority for 47% of organizations, and communications is one of the biggest generators of the data AI models now consume through transcription, summarization, and meeting agents.

An on-premises AI orchestration layer that lets a customer choose and switch which language model answers a query, and keeps that choice consistent across contact center, conferencing, and voicemail transcription, is one way in which vendors are extending the sovereignty principle into the AI layer.

IDC believes sovereignty commitments that stop at data residency and do not extend to portability and AI leave two of the newest, fastest-growing sources of risk unaddressed.

Trends

Sovereignty is shifting from a low-probability concern to a plausible reality, and several forces are accelerating the sovereignty mandate across the complete digital environment, from infrastructure to data to communications.

Multiple sovereignty pressures are converging at once:

- **Rising global regulation and cross-border dataflow fragmentation:** GDPR, NIS2, the EU Data Act, and DORA are tightening residency and lawful access rules, while diverging national policies since the Schrems II ruling complicate any single cloud control plane.
- **Government action on non-sovereign platforms:** France's 2026 decision to prohibit public sector use of Zoom, Microsoft Teams, and others shows regulators will now not only set residency rules but also restrict specific communications platforms.
- **Government action can cut off access instead of mandating it:** A June 2026 U.S. export control directive forced Anthropic to take its Claude Fable 5 and Mythos 5 models offline worldwide for weeks over foreign national access issues. The Anthropic case has a precedent in mainstream communications software: EU sanctions imposed on Russia in 2022 progressively cut off access to Microsoft Teams and Microsoft 365 for Russian-registered companies, moving from an initial suspension of new sales in 2022 to a full disconnection of existing subscriptions by 2024. These restrictions remain in force today. In both cases, it was a government directive, not the vendor's own commercial decision, that determined who could keep using the platform.
- **Challenges around sovereignty:** Many of the top challenges around communication technology solutions cited by communications and collaboration stakeholders in IDC's 2025 Enterprise Communications and Collaboration Survey are sovereignty-related, including data management issues, interoperability challenges, lack of deployment flexibility, and limited options.
- **Influence of sovereignty:** According to IDC's *Top 5 Trends in UC&C for 2026*, sovereignty is influencing UC&C deployment choices, with geopolitical uncertainty

pushing 28% of European respondents toward local providers and 25% toward sovereign network services for their communications infrastructure.

- **Business priorities:** The top two business priorities for UC&C customers are keeping the organization secure and resilient and implementing/using AI. This indicates they do not want to compromise on either area across their digital estate.
- **Audit and cloud concentration pressure:** Organizations must demonstrate traceable data flows for calls, recordings, and AI-generated content, while reliance on a few hyperscale providers narrows the room to respond as rules change.
- **Vendor concentration risk cuts both ways:** 56% of organizations name vendor lock-in as their bigger sovereignty concern, and 36% are more worried about vendor lock-out due to geopolitical uncertainty. Organizations are already acting on this, with 37% having completed a full data inventory and classification exercise to understand their exposure.

France's example and the Anthropic suspension indicate that regulations and export rules are now affecting communications platforms directly.

A related industrywide trend is adding to the pressure: AI is helping researchers find software vulnerabilities faster than before, accelerating security disclosures and patching across the communications industry in general. This raises the total cost of ownership question for every vendor, not only cloud-first ones, as more frequent updates mean more operational overhead, regardless of where the software runs.

Overall, 35% of digital-native organizations are already prioritizing complete cloud and datacenter resilience in the next 6–12 months, indicating that more digitally mature organizations treat all business-critical and data-critical workloads strategically when it comes to applying sovereignty principles.

Figure 1

Top 5 sovereignty attributes sought by organizations

- Ownership of in-country datacenter to support localization
- Country-level certifications for cybersecurity and cloud
- Sovereign controls
- Solutions to support operational resilience
- Freedom from lock-in

Source: IDC's *Digital Sovereignty Survey*, 2025

Sovereignty concerns now reach well beyond the legal team. IT, security, and AI leaders are emerging as the stakeholders most likely to raise these issues.

IT leaders and the CTO are the stakeholder group most often identified as being concerned about data sovereignty (cited by 48% of organizations), followed by AI teams at 37%.

Legal, risk, and compliance teams, the group most associated with sovereignty in the past, are now named by only 27% of organizations, behind the C-suite and board at 35% and the head of data strategy or CDO at 33%.

CISOs and security leaders follow at 33%, reflecting how close sovereignty concerns now are to security and resilience planning generally.

Vendor profile

On-premises infrastructure vendors are already among the providers organizations say they trust for data and AI sovereignty, as identified by 32% of respondents.

Mitel is headquartered in Canada, a fact the company positions as a point of trust for European buyers weighing where a vendor's ultimate corporate control sits. Its architecture is designed to keep core communications resident in the customer's own infrastructure, extending upward into the cloud only for optional capability, treating control and autonomy as a starting design principle rather than a feature layered on afterward. This differs from the more common pattern of adding sovereignty features onto a commercial cloud and security stack through contractual language and regional datacenters alone, which asks buyers to take control claims largely on faith.

Mitel WX is built around a flexible deployment model that lets customers choose or combine private infrastructure, whether Mitel Edge or their own existing infrastructure, with private cloud, and evolve that mix over time rather than committing to one model upfront. Mitel Edge is the company's approach of layering the customer premises into its architecture, the point where core communications control sits before anything optionally extends upward into the cloud. It reflects an inverted design logic: Rather than building a cloud core and adding an on-premises gateway for resilience, Mitel anchors control at the customer's own site and treats cloud connectivity as the addition, not the foundation. Core features run inside a customer-controlled environment, which is intended to embed resilience and remove a single point of failure, while add-ons such as Mitel Administration and Workflow Studio let organizations componentize the UC architecture instead of adopting it as a fixed bundle. This places Mitel WX in the third of the three deployment patterns IDC observes in the market: an architecture where UC functionality itself, not just a gateway, resides in customer infrastructure, ensuring that the customer, not the cloud provider, has the final say over where data and control sit.

From a sovereignty design perspective, several aspects of the platform stand out:

- Encryption at rest and in transit is standard across Mitel's products. Because customers already have root access to their own infrastructure, integration with customer-hosted hardware security modules has not been a priority, as they can generate and retain their own keys.
- Core telephony is designed to keep working if the connection to Mitel's cloud is cut, without falling back to a reduced survivability mode.
- A large partner and marketplace ecosystem lets customers add specialized capabilities (e.g., a sector-specific application) without being locked into a single vendor's road map for every feature.
- Customers can keep voice communications inside Mitel's sovereign platform while still using a video tool such as Microsoft Teams through a Mitel-built plug-in. This reflects the approach of integrating with tools organizations already use, so that no wholesale replacement is required.

- Many hybrid capabilities are included as part of Mitel's existing software assurance and renewal program at no additional premium, although AI services are priced separately.
- Software bills of materials are already produced for customers who ask, and Mitel is preparing for the EU Cyber Resilience Act's software certification requirements, due in the fourth quarter of 2026.

Challenges

Mitel's premises-rooted heritage means its sovereignty story is less familiar to buyers who equate modernity with public-cloud-first platforms, which can require more explanation in a competitive process than a single cloud pitch.

Certification status varies by requirement and must constantly be updated in response to evolving regulations, whether the EU Cyber Resilience Act or schemes such as Germany's C5 or the JITC in the US.

Selling primarily through a partner channel introduces its own complexity around SLAs and shared responsibility, since no single, unified commitment typically covers an entire blended solution end-to-end.

Premises-based deployments have historically been perceived as more expensive to run than cloud alternatives, a perception Mitel is working to overcome through simpler installation and management tooling.

IDC believes none of these four challenges is architectural. Instead, they are challenges of familiarity, documentation, and perception, and IDC's experience across the sovereignty market suggests all are addressable within a normal procurement cycle without a fundamental redesign. Buyers unfamiliar with a premises-rooted vendor should ask for the same architectural details they would expect from a cloud-first pitch; the unfamiliarity tends to decline quickly once the two are compared on data residency and control rather than on brand recognition. IDC already sees savvy organizations maturing their cloud strategies from "cloud first" in the last decade to "cloud smart" this decade for the right blend of control and agility.

Beyond that, certification gaps are a timing issue, not a capability gap. IDC recommends that tech buyers request a written certification road map before dismissing a vendor for a requirement still in progress across the industry. Partner-delivered SLAs are manageable with clear accountability mapping at the contract stage, a standard step in any multivendor procurement.

IDC's own data shows that total cost of ownership increasingly favors vendors that invest in patch automation and simplified management, as the operational overhead of frequent security updates, not the deployment model itself, is now the larger cost driver. Addressed early, each of these challenges becomes a procurement checklist item that need not cause delay. Shifting the conversation to value and business impact metrics also helps address cost concerns.

Conclusion

Organizations that treat sovereignty as a storage and infrastructure checkbox will keep missing the communications layer, where the same regulatory and geopolitical pressures apply but far less scrutiny currently exists. Those that extend the same discipline to calls, meetings, chat, and the AI-generated content layered on top of them will build the resilience, control, and commercial flexibility that a modern, distributed enterprise now needs.

IDC predicts that by 2027, 65% of multinational enterprises will actively reevaluate technology services partners based on their ability to offer sovereign solutions for data and cloud, a separate signal from the 65% investment increase in modular, sovereign-ready cloud environments IDC expects by 2028. Read together, the two point to the same conclusion: Sovereignty is becoming a standing procurement criterion, not a one-time evaluation.

IDC believes the market for sovereignty-aware communications architecture will continue to grow in importance. To the extent that vendors such as Mitel can address the architectural, portability, and certification challenges described in this IDC Spotlight, they have a meaningful opportunity to differentiate with sovereignty-minded buyers.

Tech buyer recommendations include the following:

- **Extend the sovereignty review to communications:** Apply the same rigor already used for storage and infrastructure to calls, meetings, chat, and the AI-generated content layered on top of them. Ask where this data physically resides, who can access it, and whether operations continue if a provider connection is lost, before evaluating any vendor's sovereignty claims.
- **Measure progress through resilience and portability, not residency alone:** Track operational metrics such as how quickly communications recover from a disrupted provider connection, how much of the estate can be exported and reimported without a rebuild, and how many sovereignty-relevant workloads have a documented owner. These are better indicators of readiness.
- **Frame the budget case around resilience and flexibility, not fear:** Position sovereignty investment as a way to reduce dependency on a single provider and preserve negotiating leverage, and avoid presenting it as insurance against a worst-case scenario. The majority of organizations are already increasing governance and resilience budgets for 2026, so this framing has board-level precedent to draw on.
- **Plan for a multi-year journey:** Sovereignty maturity builds incrementally, starting with data classification and a single high-risk workload before expanding deployment choice and portability testing across subsequent budget cycles. Treating it as a destination rather than a continuous discipline is why some initiatives stall.
- **Bring IT, security, AI, and procurement into the decision together:** IDC's data shows IT leaders and AI teams, not only legal and compliance, are now most likely to raise sovereignty concerns. Communications platform decisions should involve this broader group from the outset.

About the IDC analyst



Archana Venkatraman
Senior Research Director

Archana Venkatraman leads IDC's European CloudOps and governance research, as well as its cloud data management research.

As part of the CloudOps focus, Archana analyzes the multicloud management and operations market, cloud economics and FinOps, observability, cloud consolidation, and cloud governance and control. Significant focus areas of her research include cloud value realization, cloud-native success, and operational excellence.

More about Archana Venkatraman

Message from the sponsor

Mitel provides communications solutions for organizations operating under strict data residency, auditability, and continuity requirements. As outlined in this IDC Spotlight, sovereignty considerations that have long applied to cloud infrastructure and storage now extend to calls, meetings, chat, and the AI-generated content they produce. Mitel's approach is built on a distributed architecture that keeps core communications functionality resident within customer infrastructure, with cloud services available as an optional extension instead of a structural dependency. This gives organizations in finance, government, healthcare, and other regulated sectors a path to modernize communication while retaining control over where data resides, who can access it, and how operations continue if a provider connection is disrupted.

To learn more about Mitel's approach to sovereignty-ready communications, visit mitel.com. Contact a Mitel representative to discuss your organization's requirements.

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is 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 Research, Inc.

One Beacon Street, Suite 33100, Boston, MA 02108, USA

T +1 508 872 8200

blogs.idc.com | LinkedIn @IDC | www.idc.com

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 make fact-based technology decisions and achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA