April 2026
InfoBrief
Sponsored by Microsoft and Accenture

Sovereignty as Strategy

Enabling AI and Resilience in EMEA Cloud Ecosystems

Stuart Wilson
Senior Research Director,
EMEA Partnering Ecosystems IDC

Andreas Storz
Senior Research Manager,
EMEA Partnering Ecosystems, IDC

Table of contents

Click any title to navigate directly to that page.

In this InfoBrief

Sovereignty has moved rapidly from a compliance obligation to a strategic imperative as EMEA organizations accelerate AI adoption against a backdrop of regulatory fragmentation, geopolitical uncertainty, and rising board-level scrutiny. Organizations increasingly seek cloud and AI models that provide verifiable control, transparency, and resilience while still accessing global innovation at speed.

This InfoBrief is designed for senior leaders and cross-functional stakeholders across EMEA – including CIOs, CISOs, data, risk, legal, policy, and transformation teams – who are shaping or refining their organization's sovereignty strategy. It provides clear guidance on how to align cloud, data, AI, and operating models to build trusted, sovereign-aligned architectures that unlock innovation without compromising assurance.

> Organizations have the right to control their destiny, but not at the cost of innovation and global collaboration.

Samer Abu-Ltaif
President, Microsoft Europe, Middle East & Africa (EMEA)

Executive summary

As geopolitical uncertainty, regulatory fragmentation, and accelerated AI adoption reshape the digital landscape, sovereign cloud has moved from a compliance consideration to a strategic priority for organizations across EMEA. Enterprises increasingly require cloud and AI environments that provide verifiable control over data, infrastructure, and operations while preserving access to global innovation and scalable digital capabilities. As a result, sovereignty is becoming a **core design principle for cloud architectures and modernization strategies.**

Organizations are responding by adopting **sovereign-by-design approaches** that embed residency controls, identity boundaries, encryption, governance, and operational safeguards directly into cloud and AI environments. These capabilities allow enterprises **to align sovereignty requirements with workload sensitivity, regulatory exposure, and industry-specific risk profiles** while enabling continued modernization and AI adoption. Flexible deployment models, including public cloud with sovereign controls, managed sovereign environments, and isolated sovereign infrastructures, allow organizations to **balance control, compliance, and innovation.**

However, achieving sovereignty at scale requires more than technology choices. Many organizations face significant operational challenges, including architectural fragmentation across hybrid and multicloud estates, skills gaps in emerging areas such as AI governance and policy-as-code, and the complexity of coordinating sovereignty requirements across legal, security, and technology teams. As a result, ecosystem collaboration between cloud providers, transformation partners, and customers is becoming increasingly important to **translate sovereign architecture principles into repeatable enterprise capabilities.**

Organizations that successfully operationalize sovereignty as part of broader cloud and AI modernization strategies can strengthen resilience, maintain regulatory confidence, and accelerate the adoption of trusted AI. In this context, sovereignty is emerging not only as a mechanism for compliance but also as a **strategic enabler of secure innovation and long-term digital competitiveness.**

Sovereignty moves from constraint to strategy

Sovereignty is reshaping cloud and AI decision-making across EMEA as organizations modernize their technology estates and seek to balance innovation with rising expectations around control, compliance, security, and resilience.

- As AI adoption accelerates and geopolitical and regulatory pressures intensify, sovereignty is becoming a strategic design principle, not just a compliance requirement.
- Buyers now prioritize verifiable, customer-configurable security controls, including customer-managed encryption, identity isolation, and operational transparency aligned to workload sensitivity and sector risk.
- Jurisdictional fragmentation is driving sovereignty-aligned multicloud strategies that combine global innovation with localized assurance.
- Sovereign-by-design architectures and AI governance are emerging as the foundation for secure, responsible AI-led transformation.
- Ecosystem partnerships that combine secure cloud platform scale with enterprise transformation expertise are critical to operationalizing sovereignty at scale.

> Sovereignty is not a trade-off with innovation – it's about giving every organization real agency and trusted choices."
>
> **Samer Abu-Ltaif**
> **President, Microsoft Europe, Middle East & Africa (EMEA)**

> The hardest part isn't choosing sovereign technology – it's industrializing sovereignty across the enterprise without losing speed."
>
> **Mauro Macchi**
> **CEO, Europe, Middle East & Africa (EMEA), Accenture**

Sovereignty investment as a foundation for stability and risk mitigation

Compliance with legislation and industry regulations continue to be key drivers for ongoing investments in sovereign technologies. However, organizations across EMEA are allocating more resources to sovereign cloud solutions to strengthen resilience amid **rising geopolitical, regulatory, and economic uncertainty.** These increased investments allow enterprises to position themselves more effectively for potential disruption, ensuring they can mitigate risk, maintain continuity, and operate on solid, compliant foundations as AI adoption accelerates and jurisdictional demands grow.

- 2 in 5 EMEA customers (40%) already use **sovereign public cloud solutions,** while another 40% have plans to use them.
- Half of EMEA customers (48%) say their organization's **interest in implementing digital sovereignty solutions has increased** due to recent geopolitical uncertainties – including trade tensions, regional conflicts, and regulatory shifts.
- Globally, IDC predicts that **sovereign cloud spending will more than triple** between 2024 and 2029, growing from $126 to over $400 billion.

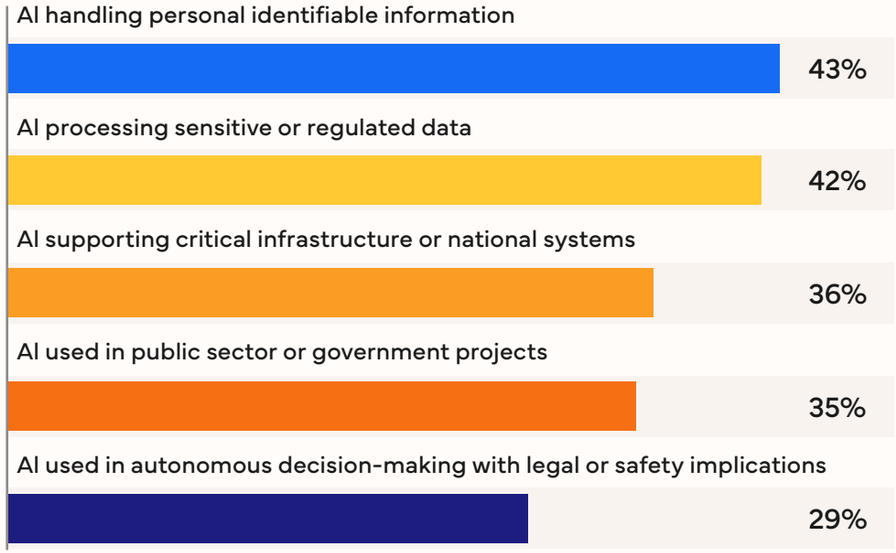
Source: IDC Europe, WW Digital Sovereignty survey 2025, July 2025. EMEA only n = 495; IDC Worldwide Sovereign Cloud Forecast, 2025–2029, December 2025, IDC #US53930025

Trusted AI depends on sovereign foundations

The rise of AI is driving increased interest and investment in sovereign cloud. Customers across EMEA seek to benefit from technological innovation and use AI for greater efficiency and business model transformation. But AI's dependency on high quality data and growing autonomous capabilities mean customers need to have the right foundations in place to deploy AI responsibly and securely. Sovereign cloud technologies enable customers to benefit from innovation while remaining compliant and in control of their data, assets, and operations.

- 43% of customers in EMEA already employ **sovereign cloud to build AI solutions,** and a further 22% plan to do so in the next 12 months. [n=401]
- 61% of organizations in EMEA say that they are more likely to adopt sovereign cloud services for AI workloads in the wake of **recent geopolitics events** – especially trade tensions, regional conflicts, and regulatory shifts. Nearly half (48%) plan to increase their use of sovereign cloud for AI workloads.
- The need for sovereign cloud infrastructure varies across **AI use cases.** EMEA customers see the strongest need for sovereign controls whenever use cases involve (1) personal identifiable information or otherwise sensitive/regulated data, (2) public sector/government projects or critical infrastructure, and (3) autonomous decision-making with safety implications.

Top 5 AI use case types for which EMEA organizations believe it is important to use sovereign cloud infrastructure

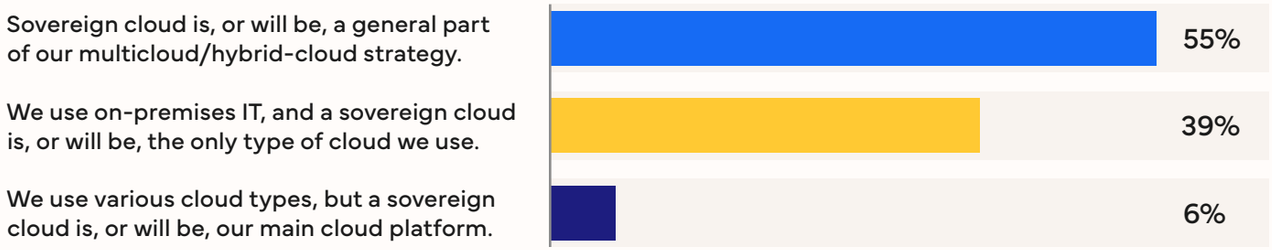


Source: IDC Europe, WW Digital Sovereignty survey 2025, July 2025. EMEA only n=262

Different needs, different sovereign models

- **Sovereign cloud is not "all-or-nothing".** While there is strong interest and projected growth, most EMEA customers will leverage sovereign cloud technologies as part of a wider multicloud / hybrid-cloud strategy.
- Different **flavors of sovereign cloud** address different levels of sovereignty requirements – ranging from public cloud with sovereign controls, over independently managed sovereign environments to entirely isolated environments running in sovereign data centers.
- An **assessment across different workloads** for regulatory requirements, data sensitivity, and risk levels should guide the selection and prioritization of appropriate deployment models and cloud strategies.
- Choice across models enables customers to **adapt to evolving regulations, risks, and requirements** based on their technology strategies.

Q: How does sovereign cloud fit into your organization's cloud strategy?



Source: IDC Europe, WW Digital Sovereignty survey 2025, July 2025. EMEA only n=495

Three Common Flavors of Sovereign Cloud

Public cloud with sovereign controls: Customer-managed platform controls (data cy, encryption/key management, access).

Sovereign managed cloud: Provider with a local trusted partner independently administering sovereign controls and enforcing local operational access.

Isolated hosted sovereign cloud: Dedicated/private cloud delivered from sovereign datacenters by partners.

Source: IDC's Worldwide Sovereign Cloud Taxonomy, 2024

Sovereignty priorities: control, compliance, personalized security, and local resilience

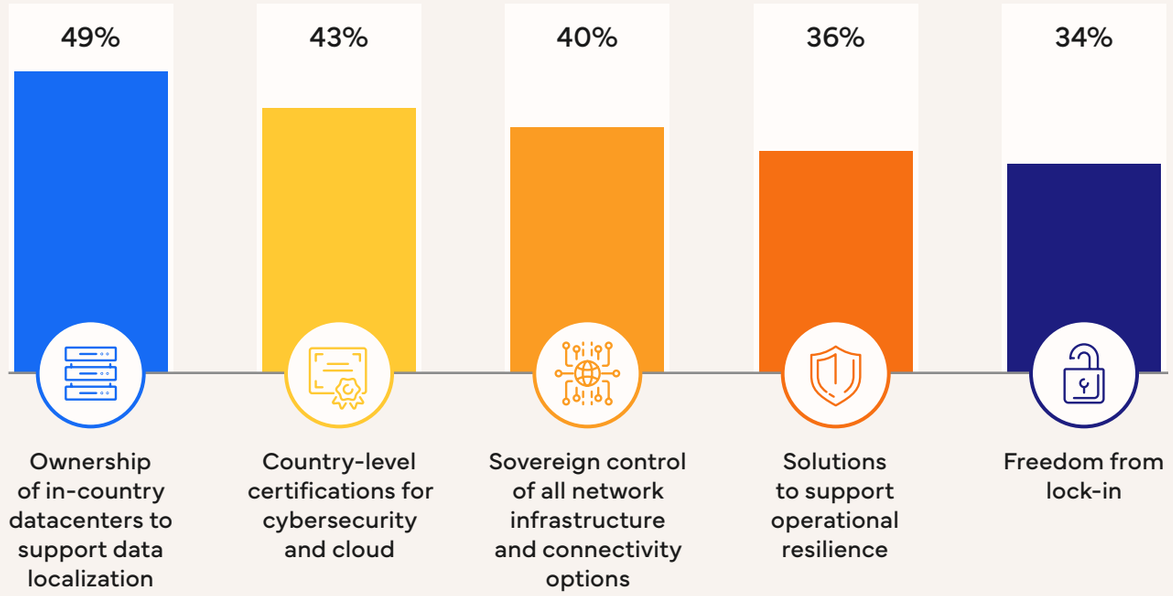
Organizations in EMEA are prioritizing sovereign cloud solutions that deliver verifiable security, strong compliance guarantees, and full data-residency control, supported by transparent operational assurance.

They increasingly require granular, customer-configurable security capabilities tailored to sector mandates and workload sensitivity.

Providers are evaluated not only on local availability and resilience, but on their ability to deliver secure-by-design, cloud-native architectures that support AI modernization without increasing complexity.

As sovereignty becomes a board-level mandate, organizations seek consistent governance, jurisdictional clarity, and security personalization across increasingly distributed multicloud estates. These foundations form the secure base from which trusted, compliant, and high-performing AI capabilities can scale.

Q: Which attributes are important when choosing a sovereign cloud partner or provider? [Choose all that apply]



Source: IDC Europe, WW Digital Sovereignty survey 2025, July 2025. EMEA only n=495

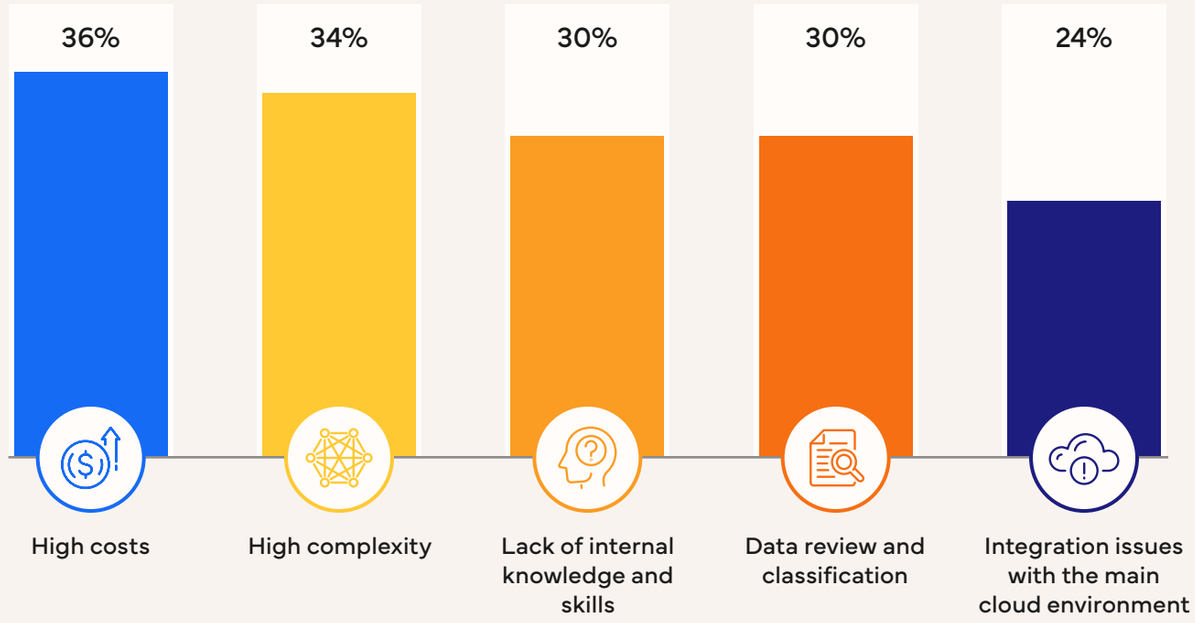
Sovereignty challenges demand smart prioritization

High costs, complexity, and skills gaps show that organizations cannot apply sovereign cloud uniformly across all workloads. Integration and data-classification challenges further reinforce the need to **prioritize sovereignty by use case and sensitivity.**

EMEA organizations increasingly benefit from working with trusted partners who can assess workload-level requirements, streamline decisions, and **determine where sovereign controls are essential - and where they aren't.**

> One of our most important findings has been that only about one-third of AI workloads need to be sovereign."
>
> **Mauro Macchi**
> **CEO, Europe, Middle East & Africa (EMEA), Accenture**

EMEA customers' top challenges in implementing sovereign cloud



Source: IDC Europe, WW Digital Sovereignty survey 2025, July 2025. EMEA only n=495

Sovereign-by-design makes control consistent and scalable

Sovereign-by-design turns sovereignty from a one-time compliance response into an engineered, security-first enterprise capability that scales across jurisdictions and workloads. This transforms sovereignty from reactive compliance into an engineered, consistent, and repeatable capability that can scale across jurisdictions, workloads, and evolving regulatory demands.

- Sovereign-by-design architectures embed residency, encryption, identity isolation, zero-trust access controls, auditability, and operational safeguards directly into the cloud stack. This approach makes security configurable by jurisdiction, industry mandate, and workload sensitivity rather than retrofitted through overlays or exceptions.
- By integrating policy-as-code, continuous compliance, and automated governance controls, sovereign-by-design enables organizations to enforce residency, access boundaries, and AI governance requirements consistently across hybrid and multicloud environments.
- Critically, it allows enterprises to apply sovereign controls selectively, strengthening protection where data sensitivity or AI risk is highest, while avoiding unnecessary complexity in lower-risk workloads. This balance supports modernization at speed while preserving assurance.
- As organizations embed AI into core operations and modernize legacy estates, sovereign-by-design becomes the architectural foundation for secure, responsible, and scalable AI-driven transformation.

> “Sovereignty is not a zero-sum problem. Platforms need to be engineered with trust, compliance, security, and resilience built in.”
>
> **Samer Abu-Ltaif**
> **President, Microsoft Europe, Middle East & Africa (EMEA)**

> “Sovereign-by-design turns sovereignty from a one-time compliance event into a repeatable enterprise capability.”
>
> **Mauro Macchi**
> **CEO, Europe, Middle East & Africa (EMEA), Accenture**

Designing an AI-ready sovereign cloud

An AI-ready sovereign cloud is not simply a compliance construct. It is the modernization platform that enables organizations to embed AI into core operations while maintaining control, security, and regulatory assurance. As enterprises modernize applications, data estates, and operating models, sovereignty must extend consistently across the entire AI lifecycle.

Organizations increasingly require architectures that support multiple sovereignty levels aligned to workload risk, regulatory exposure, and sector sensitivity. This includes the ability to configure security postures such as customer-managed keys, role-based access controls, and jurisdiction-specific operational boundaries according to AI use case criticality.

By embedding policy-as-code, continuous compliance monitoring, and auditable AI operations, enterprises can scale AI responsibly while maintaining confidence in governance, explainability, and resilience. As AI systems become more autonomous and business-critical, sovereign cloud capabilities form the secure foundation for sustainable, large-scale AI transformation.

AI-ready sovereign cloud requirements

- **End-to-end control of AI data, models, and pipelines:** Enforces data-residency, identity boundaries, encryption, and access governance across the entire AI lifecycle – from training datasets to inference outputs.
- **Configurable security and operational boundaries:** Supports customer-managed keys, privileged access controls, policy-as-code, and jurisdiction-specific operational oversight tailored to workload sensitivity.
- **Assurance for responsible and auditable AI:** Embeds continuous compliance, monitoring, and traceability so AI operations meet regulatory, sector, and ethical obligations.
- **Flexible sovereignty models for AI deployment:** Enables AI workloads to run across public cloud with sovereign controls, managed sovereign environments, or isolated sovereign clouds aligned to risk and modernization objectives.

> “Every organization needs the ability to shape its own future. Sovereignty starts with agency.”
>
> **Samer Abu-Ltaif**
> **President, Microsoft Europe, Middle East & Africa (EMEA)**

Untangling complexity to build an enterprise-wide sovereignty strategy

Sovereignty decisions often stall because organizations face fragmented architectures, misaligned decision rights, siloed teams, and uneven capabilities, making it difficult to form a unified strategy. These constraints lead to inconsistent controls across workloads and cloud environments. Experienced third-party partners help organizations cut through internal complexity, assess sovereignty needs by workload, and build a repeatable, enterprise-wide framework that overcomes resistance and drives consistent implementation.

- Many organizations struggle because sovereignty spans data, identity, infrastructure, and governance layers, requiring coordinated change far beyond IT alone. This cross-stack complexity slows clarity and execution.
- Fragmented ownership across legal, risk, security, and technology creates strategic drift; without aligned decision rights, sovereignty remains a compliance task rather than an enterprise capability.
- Trusted partners bring outside perspective and structured methods to assess workload sensitivity, harmonize controls, and build repeatable sovereignty patterns that scale across business units and cloud estates.

> “The biggest challenge we see is that sovereignty cuts across the entire stack - it’s not one decision, it’s an operating system change.”
>
> **Mauro Macchi**
> **CEO, Europe, Middle East & Africa (EMEA), Accenture**

Scaling sovereignty through managed expertise

Designing and operating sovereign cloud environments can overwhelm individual organizations due to fragmented architectures, varying regulatory obligations, and limited internal expertise. Managed sovereign-cloud partners bring structured methods, local regulatory understanding, and cross-industry experience to harmonize controls across data, identity, and operations. By providing ongoing governance, workload mapping, and operational assurance, these partners help organizations create a repeatable, enterprise-wide sovereignty model that accelerates adoption and reduces risk.

- 2 in 3 EMEA customers either already use (32%) **managed sovereign cloud** infrastructure and platform delivered together with a local partner or plans to use it in the next 12 months (34%) .
- Managed sovereign-cloud providers help unify governance across data, identity, and infrastructure, overcoming inconsistent controls that emerge when multiple teams interpret requirements differently
- Their regulatory awareness and local market insight ensure sovereignty decisions reflect sector-specific rules, jurisdictional boundaries, and risk exposure, strengthening confidence in deployment choices.
- External partners deliver structured, repeatable patterns that scale across business units, breaking down silos and reducing the operational burden of maintaining sovereignty at enterprise level.

Source: IDC Europe, WW Digital Sovereignty survey 2025, July 2025. EMEA only n=300

The power of the ecosystem: Three parties, one shared vision

Sovereignty at scale requires more than technology. It demands alignment between secure cloud platforms, enterprise transformation capabilities, and customer strategy. Microsoft and Accenture combine platform-level sovereign-by-design engineering with operational modernization expertise to help organizations translate sovereignty into measurable business outcomes.

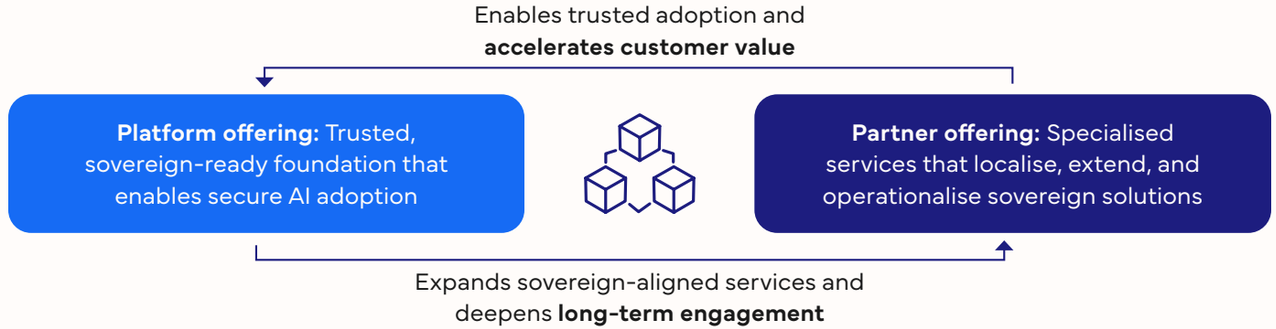
Ecosystem-enabled sovereignty creates a structured, three-way value dynamic:

Platform offering delivers secure, AI-ready cloud platforms engineered with sovereign-by-design principles, enabling configurable security controls, compliance assurance, and global innovation at scale.

Partner offering industrializes sovereignty across the enterprise aligning governance, operating models, application modernization, and AI adoption to sector-specific regulatory and risk requirements.

Customers gain the ability to modernize securely, scale AI responsibly, and adapt sovereignty postures as regulations, risks, and geopolitical conditions evolve.

When secure platform engineering and enterprise transformation expertise converge, sovereignty shifts from a constraint to a strategic enabler. This ecosystem approach reduces operational complexity, accelerates modernization, and embeds personalized security controls consistently across cloud, data, and AI environments.



> Sovereign-by-design creates resilience and keeps innovation moving – because governance becomes engineered, not renegotiated every time."
>
> **Mauro Macchi**
> **CEO, Europe, Middle East & Africa (EMEA), Accenture**

Business benefits: Sovereignty as a strategic advantage

When sovereignty is treated as a strategic design principle rather than a compliance obligation, it becomes an **enabler of secure modernization and AI-driven transformation.**

Greater control does not restrict innovation. It accelerates it. By embedding configurable security controls, identity boundaries, and governance mechanisms into cloud and AI architectures, organizations create the confidence required to modernize core systems, migrate sensitive workloads, and **operationalize AI at scale.**

- Sovereign-aligned cloud strategies enable enterprises to:
- Accelerate application and data modernization while maintaining jurisdictional clarity
- Scale AI adoption securely across regulated and high-sensitivity environments
- Reduce operational risk through consistent, policy-driven security enforcement
- Adapt quickly to evolving regulatory, geopolitical, and sector-specific requirements

Organizations that operationalize sovereignty gain more than compliance assurance. They establish a resilient foundation for innovation, faster time to value from AI investments, and sustained competitive differentiation in increasingly complex digital ecosystems.

> When sovereignty is treated as an enabler of trust everyone benefits.
>
> **Samer Abu-Ltaif**
> **President, Microsoft Europe, Middle East & Africa (EMEA)**

> The inflection point is when sovereignty becomes an advantage strategy, not a risk strategy.
>
> **Mauro Macchi**
> **CEO, Europe, Middle East & Africa (EMEA), Accenture**

Actions to strengthen your sovereignty strategy

Prioritize by workload risk and AI impact

Classify data sensitivity, regulatory exposure, and AI criticality to apply sovereign controls where they matter most.

Build sovereignty into modernization from day one

Embed residency, encryption, identity isolation, and policy-as-code into cloud migration, application modernization, and AI programs.

Govern the full AI lifecycle

Extend security, compliance, and auditability from data ingestion to model deployment and inference.

Enable configurable security at scale

Adopt customer-managed keys, access governance, and jurisdiction-specific controls that adapt as risks and regulations evolve.

Industrialize sovereignty across the enterprise

Leverage ecosystem expertise to reduce complexity, harmonize controls, and accelerate secure, AI-driven transformation.

Elevate sovereignty to a board-level modernization strategy

Position sovereignty not as a compliance overlay, but as the secure foundation for resilient, AI-enabled growth.

About the IDC analysts

Stuart Wilson

Senior Research Director, EMEA Partnering Ecosystems IDC

Stuart Wilson is senior research director for IDC's Europe, Middle East & Africa (EMEA) Partnering Ecosystems program. With over two decades of global experience, Stuart focuses on the rise of complex, connected ecosystems and how platform models are reshaping routes to market and partner engagement frameworks.

More about Stuart Wilson →

Andreas Storz

Senior Research Manager, EMEA Partnering Ecosystems, IDC

Andreas Storz is senior research manager for IDC's Europe, Middle East & Africa (EMEA) Partnering Ecosystems program. Based in the US, Andreas focuses on the evolution of go-to-market models, new digital value chains and the wider impact on partner ecosystems, exploring how current and future trends will impact the vendor, distributor, and partner landscape.

More about Andreas Storz →

Message from Microsoft and Accenture

Samer Abu-Ltaif
Microsoft | EMEA President Senior Regional Leadership

Sovereignty has entered a new phase across EMEA. It is no longer viewed simply as a regulatory obligation, but as a strategic foundation for resilience, trust, and long-term digital transformation. The IDC InfoBrief reflects a clear shift in customer priorities. Sovereignty is increasingly being designed into technology decisions from the outset, shaping how organizations modernize their estates and prepare for AI-driven growth. This reinforces a fundamental reality we see across the region: innovation and control are not trade-offs, they must advance together. Microsoft's approach is built on choice and accountability, enabling organisations to align sovereignty requirements with workload sensitivity, risk, regulatory expectations and business continuity - while continuing to innovate at scale. Crucially, responsible AI innovation depends on strong guardrails. Organizations should not embark on their AI journey without the foundations of compliance, security, federation, and data access firmly in place. That is why close collaboration - with regulators and trusted partners - is essential. When sovereignty is embedded by design, it becomes an enabler of trusted AI adoption and sustainable growth.

Mauro Macchi
Accenture | EMEA CEO

As organizations across EMEA accelerate AI adoption, sovereignty has emerged as a strategic foundation for resilience, trust, and long-term value creation. As this IDC InfoBrief highlights, leading enterprises are moving beyond sovereignty as a mere regulatory requirement, instead embedding it as a core design principle across their cloud, data, and AI architectures. Accenture is committed to helping organizations operationalize these "sovereign-by-design" approaches across increasingly complex, multi-cloud environments. By combining secure, AI-ready cloud platforms with deep industry expertise and transformation capabilities, Accenture and technology partners such as Microsoft enable clients to align sovereignty requirements with specific workload risks and business priorities—while preserving choice, flexibility, and access to a broader ecosystem. We empower organizations to achieve trusted AI adoption without compromising the pace of innovation. This InfoBrief is designed to support executive level strategies for transforming sovereignty from a compliance constraint into a scalable enterprise capability—one that strengthens digital confidence, operational resilience, and AI-led growth.

Mark Chaban
Microsoft | EMEA VP Commercial Cloud Solutions

Sovereignty has become one of the defining leadership questions for organizations across Europe, the Middle East, and Africa. As AI adoption accelerates and geopolitical and regulatory complexity increases, we see organizations re-framing sovereignty as a strategic design choice. The most forward-looking leaders operationalize sovereignty through architecture, embedding control, transparency, and resilience directly into their cloud and AI foundations. When sovereignty is designed from the start, it becomes an enabler of responsible AI, operational resilience, and sustained growth. At Microsoft, we believe trusted innovation depends on choice, transparency, and partnership. No organization can operationalize sovereignty alone. Progress happens when platforms, partners, and customers work together to translate policy intent into practical, scalable architectures that support real-world business outcomes. This IDC InfoBrief reflects what we see every day across EMEA: sovereignty is not about constraint, it is about creating the conditions for trusted, resilient, and responsible AI-driven transformation. Leaders who approach sovereignty with clarity and intent are not just managing risk - they are building durable advantage for the years ahead.

Ihab Foudeh
Microsoft | EMEA GM Commercial Partners leadership

Sovereignty at scale cannot be delivered by technology alone. For governments and critical industries, success increasingly depends on a **strong partner ecosystem** capable of translating sovereignty principles into operational reality.

IDC InfoBrief underscores the growing importance of sovereignty as a foundation for resilience, continuity, and trust. Meeting these requirements—particularly in highly regulated and national contexts—demands close collaboration between cloud providers, local partners, and system integrators with deep regulatory and industry expertise.

Microsoft's sovereign cloud approach is designed to enable this collaboration. By combining platform-level sovereignty capabilities with trusted partners, organizations can modernize confidently while remaining aligned with national, regulatory, and operational expectations. Partners play a critical role in local delivery, compliance alignment, and long-term operational assurance.

As AI adoption accelerates, this ecosystem-driven model becomes even more important. Embedding sovereignty into cloud and AI foundations—together with partners—ensures innovation is not only scalable and secure, but also sustainable over time.

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.com @idc @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 helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.