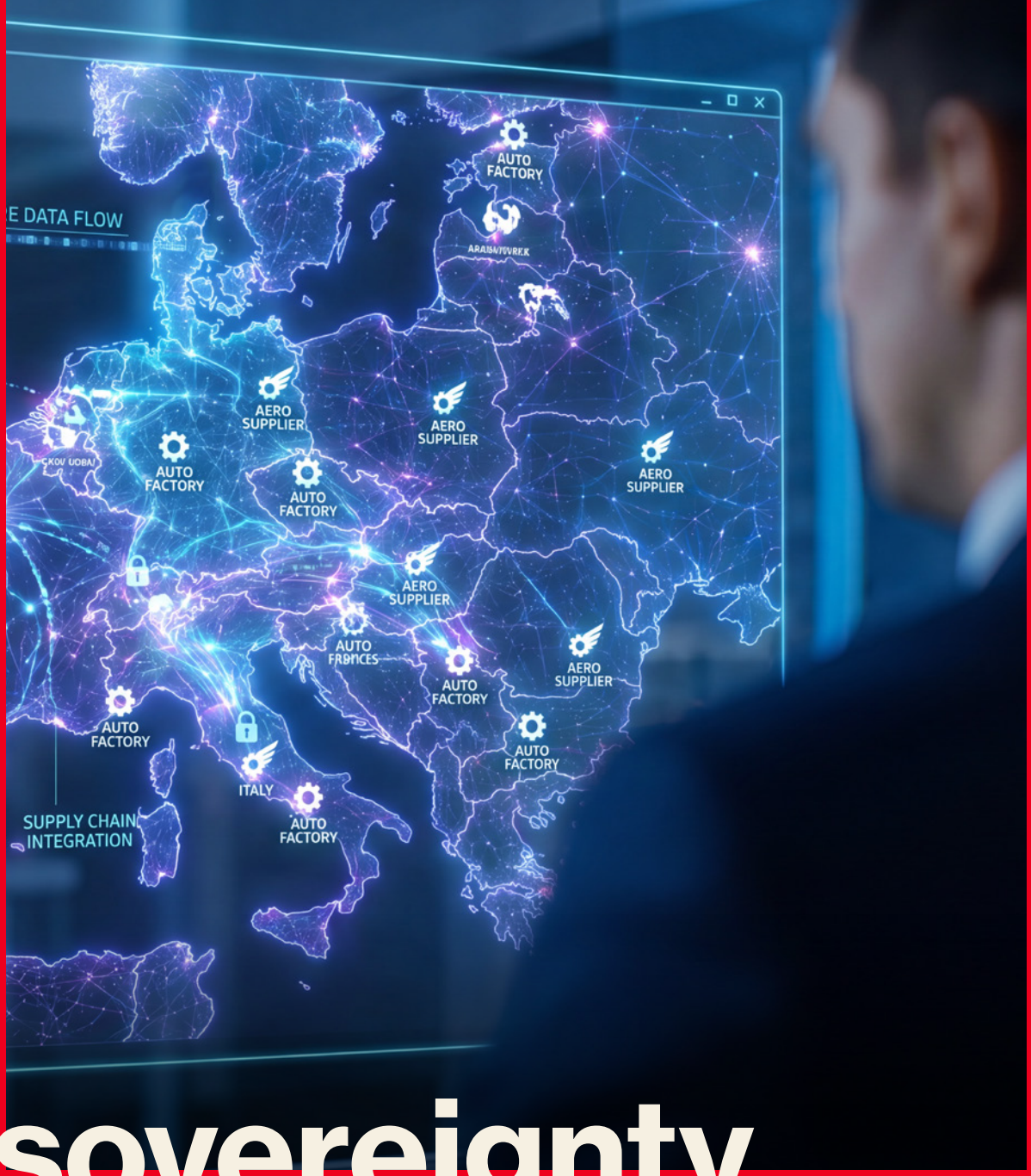
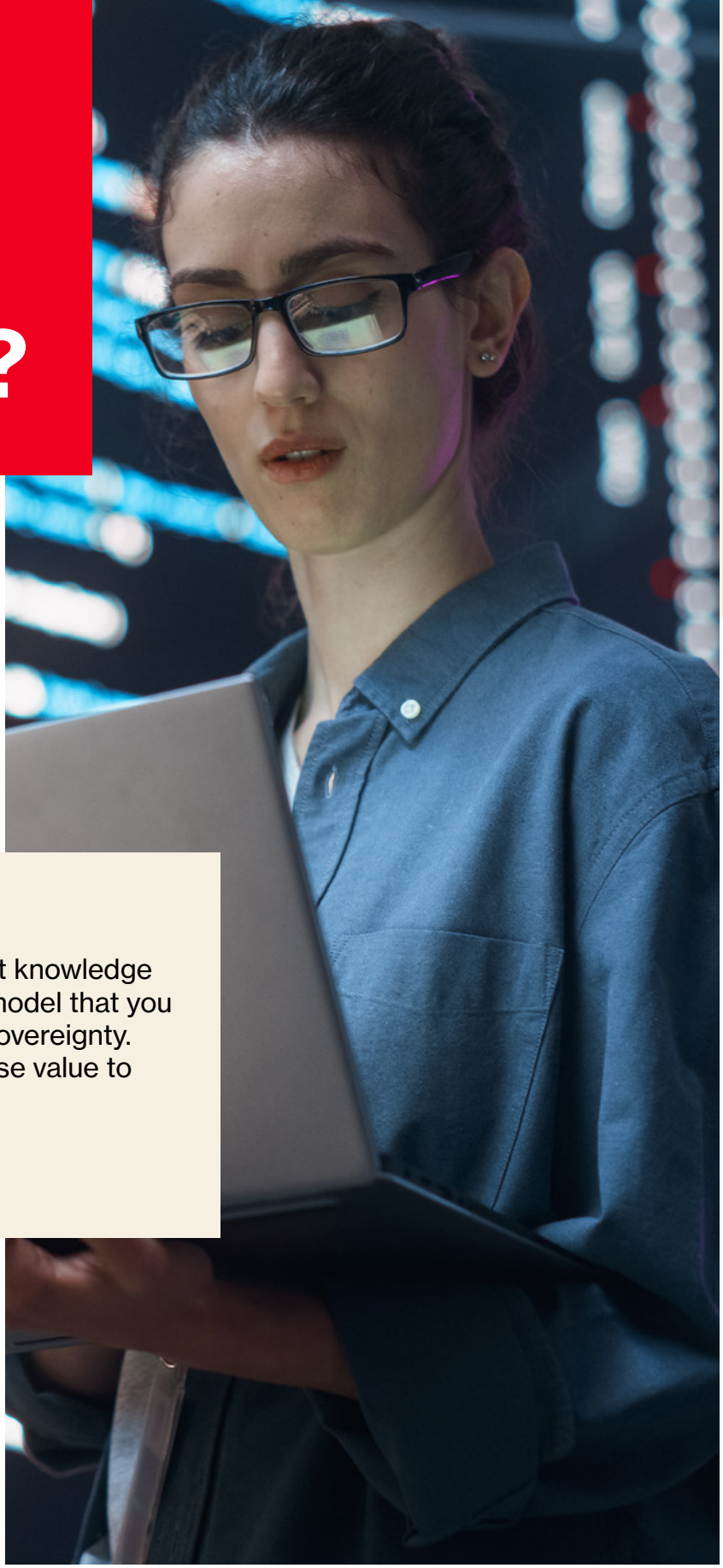


AI sovereignty

Is AI data truly secure without sovereignty?

verizon business

Is AI data truly secure without sovereignty?



In this rapidly evolving AI-driven world, organizations increasingly need to take control and eliminate risks by ensuring their valuable data and AI models remain within their strict national or regional boundaries. Defined as AI sovereignty, it is needed because modern AI systems continuously process sensitive data and proprietary models, posing complex challenges around accountability, auditability and data governance.[1]

> “If you're not able to embed the tacit knowledge of the firm in a set of weights in a model that you control, by definition you have no sovereignty. That means you're leaking enterprise value to some model somewhere.[2]”
>
> **Satya Nadella,**
> CEO, Microsoft

Sovereignty has evolved beyond merely where data resides; it now crucially concerns who manages the physical location of computational processes.[3] By decentralizing AI capabilities and removing reliance on external gatekeepers, organizations can use the help of open-source models to preserve their autonomy over data security, build operational resilience and remain competitive.

1. Stanford University, AI Sovereignty’s Definitional Dilemma, https://hai.stanford.edu/news/ai-sovereigntys-definitional-dilemma, 2026
2. The Registar, Speed: Microsoft CEO: AI sovereignty isn't where it runs, it's who controls it, https://www.theregister.com/software/2026/01/21/nadella-talks-ai-sovereignty-at-the-world-economic-forum/5128191, 2026
3. 3. Red Hat, What is Sovereign AI? https://www.redhat.com/en/topics/ai/sovereign-ai, 2026

Leaders need multi-layered AI control

In this complex and evolving environment, leaders must move past simplistic, all-encompassing notions of "control." Instead, they need to formulate a sophisticated, multi-layered strategy that deliberately addresses different aspects of their operations.[4] For example, in a Cisco report, an AI agent produced 450% more network traffic than a human executing the same task manually.[5] Therefore they may be a future requirement to separate human traffic and agentic traffic on to separate network infrastructure that may include other distinct components, such as data residency, model ownership, or operational governance, and applying tailored, intentional approaches to each.

Key concepts include:

- Territorial control: determining where data and computing resources are physically located.
- Operational control: managing and securing these critical assets.
- Technological control: owning the underlying infrastructure, algorithm and intellectual property.

> "
>
> IDC predicts that by 2028, CIOs at multinational organizations will increase investments in modular, sovereign-ready cloud and data localization environments by 65% to future-proof operations against rising sovereignty demands.[6]

4. Kyndryl, Lovejoy, he physical foundations of digital sovereignty: How to reclaim control in the age of AI, https://www.kyndryl.com/gb/en/insights/articles/2026/04/ai-sovereignty-enterprise-control, 2026
5. Cisco, AI Impact on Wide Area Networks, https://www.cisco.com/c/dam/en/us/solutions/collateral/artificial-intelligence/mass-scale-infrastructure/ai-network-traffic-report.pdf, 2026
6. IDC, Claps and Nasir, Dispelling the myth of a silver bullet in sovereign, https://www.idc.com/resource-center/blog/dispelling-the-myth-of-a-silver-bullet-in-sovereign-ai/, 2026

Trusted data transforms European supply chains

BMW stays digitally connected to their supply chain through Catena-X, a collaborative open data ecosystem in which information flows securely and in a standardized manner.[7]

BMW leverages Catena-X to boost transparency, such as calculating parts' carbon footprints and enhance resilience by detecting bottlenecks early. Pilot projects demonstrate how this initiative optimizes information flow, driving greater sustainability and efficiency across BMW's digital supply chain, ultimately transforming automotive value chains.[7]

In aviation, Airbus is creating an Aerospace Data Space to securely connect its vast network of approximately 10,000 suppliers.[8] Through the EU-backed Gaia-X data sovereignty initiative, the platform ensures sensitive operational and engineering data remains under European control, preventing vendor lock-in and fostering trust.

By adopting a federated, sovereign data model, Airbus ensures data autonomy for participants. This strengthens European aerospace resilience, security and collaboration, driving innovation while preserving digital sovereignty.

7. BMW Group, On the way to a digitally connected supply chain with Catena-X, https://www.bmwgroup.com/en/news/general/2025/catena-x-connects-digital-supply-chains.html, 2025

8. Raconteur Magee, Why Airbus is all-in on EU data project Gaia-X, https://www.raconteur.net/technology/why-airbus-is-all-in-on-eu-data-project-gaia-x, 2024

Will companies ever truly own their AI?

Shifting from paying for external AI services, especially flagship models, to deploying your own models transforms AI from an ongoing cost into a valuable strategic asset for the business. Large organizations are finding it increasingly difficult to justify their AI spending, with a number of corporate leaders having to revise their initially optimistic projections for AI—as was the case with Uber, when the company burnt through its entire 2026 AI budget in just four months.[9] This is where companies like Mistral are on a mission of democratizing artificial intelligence through open-source, efficient, and innovative AI models, products and solutions.[10]

As Hanah-Marie Darley, co-founder and CAIO at Geordie AI comments, "businesses will likely need to achieve AI sovereignty initiatives by partnering with other companies or countries as opposed to standing up their own models. Even if you can guarantee the data storage, you won't guarantee the functionality, and so you probably won't keep pace with frontier models that have billions in investment if you're trying to build them yourself."[11]

> "I can see very much being something they want to adopt because they'll have spent a lot of money on their own AI models they probably don't want to run them in the cloud it probably makes more commercial sense to run it privately and they can be a bit more confident in securing their data and their algorithms."
>
> **Colin Wilson,**
> Enterprise Architect, Verizon Business

9. Fortune, Angelo, Uber burned through its entire 2026 AI budget in four months. Now its COO is questioning whether it's worth it, https://fortune.com/2026/05/26/uber-coo-ai-spending-tokens-claude-code/, 2026
10. Matt Turck, LinkedIn Post available at: https://www.linkedin.com/posts/turck_while-silicon-valley-obsesses-over-agi-mistral-ugcPost-7427752521298821120-BLOm/, 2026
11. IT Brew, Monsanto, What is AI sovereignty and why are companies chasing after it? https://www.itbrew.com/stories/2026/04/27/what-is-ai-sovereignty-and-why-are-companies-chasing-after-it, 2026

Mastering AI Sovereignty: A multi-layered approach

Owning the infrastructure that AI sits on makes it a strategic asset, but achieving full sovereignty involves complex, multi-layered control. However, data sovereignty can't be protected by policy alone. Digital tokenization keeps systems interoperable and insights flowing, all while keeping personally identifiable or regulated information fully protected. This allows data to move freely through analytics, AI pipelines and partner ecosystems without ever exposing what's real.[12]

Why it matters

In an AI-driven world, organizations increasingly need to control their own valuable data and AI infrastructure. Without AI sovereignty, organizations face critical challenges, spiralling costs and lack of flexibility:

- Compromising accountability, auditability, and data governance for sensitive data and proprietary models.
- Risking "leaking enterprise value" if they don't control the models embedding their firm's tacit knowledge.
- Missing out on the opportunities of training AI on their own data—creating more efficient ways to action their own data.

What this means

AI sovereignty extends beyond data residency to who manages computational processes. It requires:

- Taking control by decentralizing AI capabilities and removing reliance on external gatekeepers, with digital tokenization enabling secure processing even across distributed environments.
- Some enterprises are likely to build their own full stack AI infrastructure.
- A multi-layered control strategy encompassing territorial (where), operational (how managed) and technological (owning infrastructure/IP) considerations.
- Leveraging open-source models to preserve autonomy over data security, build operational resilience and remain competitive.

[12] ALTR, AI sovereignty demands more than borders—it requires control over how data behaves. Digital tokenization is the key to that control, https://altr.com/blog/without-digital-tokenization-there-is-no-sovereign-ai/, 2026

And the consequence

Shifting to AI sovereignty transforms AI from a recurring expense into a valuable strategic asset for the business. However:

- Achieving full AI sovereignty and keeping pace with frontier models might be needed in some national security and critical infrastructure applications, but for other areas; digital tokenization becomes crucial for securely sharing insights and collaborating without compromising raw data.
- Trying to build and maintain advanced models in isolation can be functionally challenging and may not keep pace with billions in external investment.

Need to know

Leaders must develop sophisticated, multi-layered strategies for AI control beyond simplistic notions.

- CIOs at multinational organizations are predicted to increase investments in modular, sovereign-ready cloud environments by 65% by 2028, with digital tokenization being a fundamental technology for securing data flows within these controlled environments.[6]
- Companies like Mistral are democratizing AI through open-source solutions, but collaborative initiatives are key to comprehensive sovereignty.[8]

6. IDC, Claps and Nasir, Dispelling the myth of a silver bullet in sovereign, https://www.idc.com/resource-center/blog/dispelling-the-myth-of-a-silver-bullet-in-sovereign-ai/, 2026

8. Raconteur Magee, Why Airbus is all-in on EU data project Gaia-X, https://www.raconteur.net/technology/why-airbus-is-all-in-on-eu-data-project-gaia-x, 2024

Achieving AI sovereignty: What's the network impact?

Achieving full AI sovereignty, as outlined through a multi-layered approach encompassing territorial, operational, and technological control, is not merely a strategic aspiration but a practical imperative with profound operational and infrastructure implications. The following table describes how core business needs directly translate into specific AI requirements and critically, the robust network infrastructure necessary to establish and maintain comprehensive AI control.

Business need	AI need	Network impact
Ensure accountability, auditability and data governance.	Implement strict data residency and processing controls, ensuring sensitive data and proprietary models remain within defined legal safety zones.	Requires robust network segmentation, geo-fencing capabilities, and secure, encrypted private links to guarantee data localization and prevent unauthorized data transit across borders.
Prevent "leaking enterprise value" and protect intellectual property.	Securely train, deploy, and manage AI models, maintaining full technological control over algorithms, weights, and embedded tacit knowledge.	Demands high-security, isolated network environments for model development and inference, coupled with stringent egress filtering and intrusion detection to prevent intellectual property leakage and ensure model integrity.
Build operational resilience and reduce reliance on external gatekeepers.	Support decentralized AI deployments, including edge computing and federated learning, across various physical locations and sovereign cloud instances to maintain autonomy.	Necessitates a highly resilient, low-latency, and scalable distributed network architecture capable of managing diverse workloads and ensuring consistent performance across decentralized AI devices.
Help partners share data safely and consistently.	Enable controlled and auditable sharing of data and model insights with partners, ensuring each participant maintains sovereignty over their contributions, often facilitated by tokens to protect sensitive information.	To share data safely, companies need secure links, zero-trust network architecture (ZTNA) and secure API gateways for controlled data flow, plus, precise access rules, ensuring information safety and compliance.
Create a multi-layered control strategy for compliance.	Enforce distinct policies for territorial control (where), operational control (how managed) and technological control (owning infrastructure/IP).	Flexible, software-controlled networks are vital to instantly apply precise policies, manage traffic and guarantee compliance across all computing locations.
Transform AI from an ongoing cost into a valuable strategic asset.	Support in-house AI development, training and deployment, including the integration of open-source models into a sovereign ecosystem.	Shifts network resource allocation towards high-performance internal networks for vast data processing and model training, optimizing internal data transfer costs and maximizing efficiency of owned infrastructure for AI workloads.

Helping organizations implement AI sovereignty

There are undoubtedly many more steps to take on the AI road. This is true for enterprises worldwide: we are all "AI works in progress."

By prioritizing transparency, explainability and human oversight, we've learnt how to build trust in AI systems and empower employees to thrive in an AI-driven future. Our experience underscores the importance of a holistic AI sovereignty strategy that not only considers the technological aspects of AI but also the human and ethical dimensions, paving the way for a more responsible and beneficial integration of AI.

As you shift toward distributed edge and open-source models to maintain data sovereignty, your network becomes your new security perimeter. You cannot execute a distributed AI strategy without an agile, intelligent global foundation. Verizon provides the Network as a Service (NaaS) and managed secure architecture required to dynamically route shield and process your sovereign AI data exactly where it needs to be, all without sacrificing performance, speed, or compliance.

Complete autonomy and absolute sovereignty of AI might be too problematic for some industries but greater control and degrees of independence particularly for proprietary data are on many agendas.

Find out more

Understanding how to generate value from AI sovereignty and build the network to support its unique demands is essential. Verizon works with businesses globally, helping them leverage AI to accelerate innovation, enhance services, harvest insights and drive business intelligence. Learn more about how we can help you.