Arelion

Data sovereignty in practice

A survival guide for enterprises



Data sovereignty refers to the ability to control where data is stored, how it moves and which legal jurisdictions it is exposed to. That control is harder to maintain as enterprise data flows across cloud platforms, third-party networks and national boundaries.

No longer a niche concern, data sovereignty is now a core business priority across sectors, shaping how enterprise networks are designed and governed across increasingly complex environments. Arelion's 'Connecting Through Chaos' report found that 77% of leaders are heavily influenced by data sovereignty concerns when selecting a backbone network supplier.



As data flows between providers and across borders, maintaining oversight is becoming increasingly challenging, and organizations are rethinking their reliance on global cloud providers. Gartner identifies this shift as “geopatriation”[1], a top strategic trend for 2026, as organizations respond to geopolitical and regulatory pressure.

Yet execution remains difficult. Arelion’s latest research shows that 70% of leaders are losing sleep over the security of critical corporate data, while confidence drops from 52% within their own network domains to 40% across third-party environments. Nearly half of organizations (48%) are not confident they can demonstrate compliance.

The practical reality is that sovereignty depends not just on where data resides, but how it moves, and whether that movement can be understood and evidenced.



[1] https://www.gartner.com/en/newsroom/press-releases/2025-10-20-gartner-identifies-the-top-strategic-technology-trends-for-2026



Many enterprises still lack a complete view of where data resides

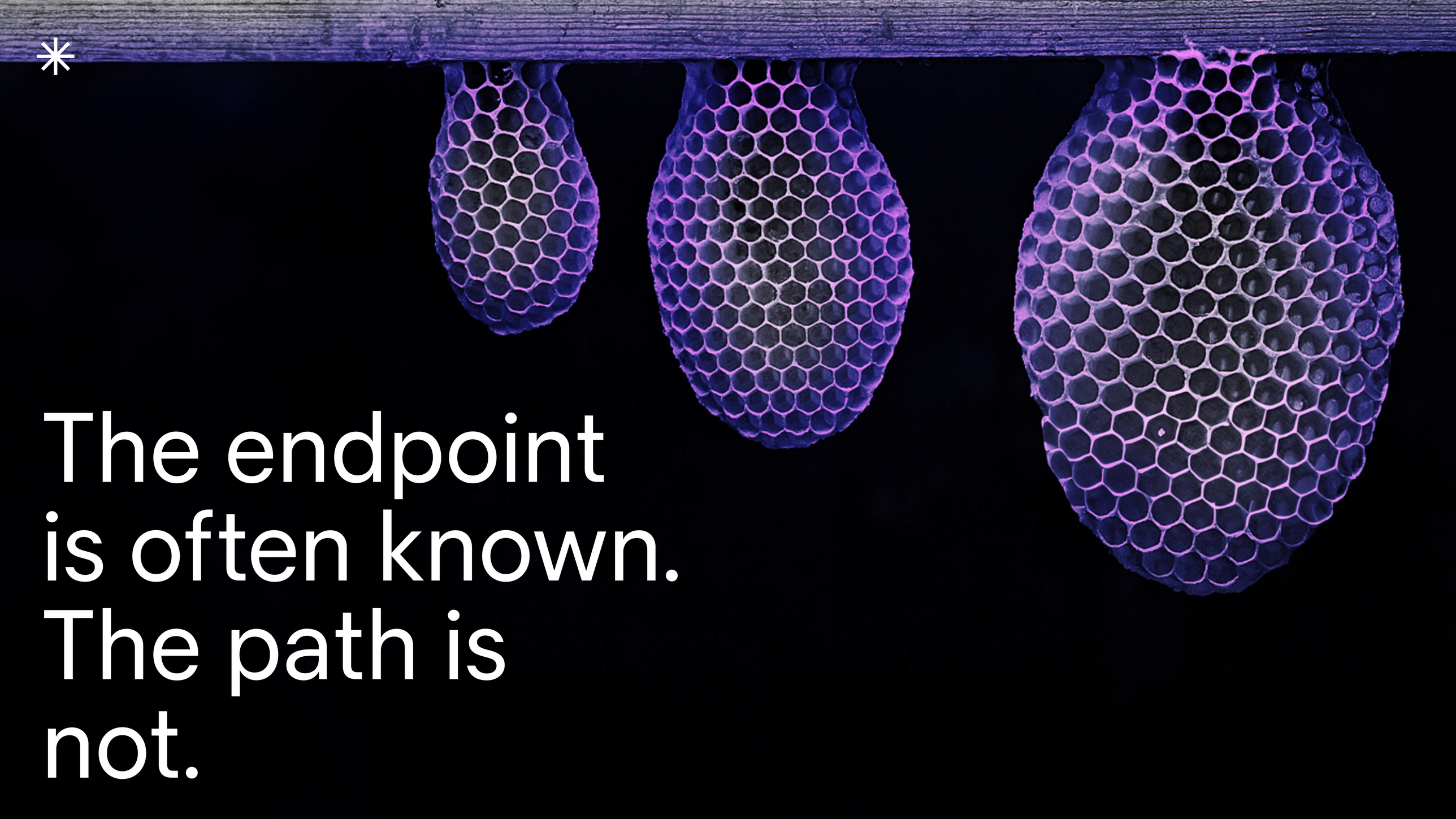
Many organizations still approach data sovereignty through location, focusing on where data is stored. In practice, that view is incomplete.

Enterprise data is now distributed by design, increasingly stored, replicated, processed and accessed across a mix of cloud platforms, private infrastructure and third-party environments. As cloud adoption has scaled, so has fragmentation, while regulatory expectations have shifted towards greater control, accountability and jurisdiction.

This creates a major visibility problem: enterprises often lack a complete picture of where their data actually resides. Arelion's research shows that strikingly, 32% of leaders are unable to identify all of their own data center locations, rising to 49% when they're using a third-party data center provider.

At the same time, AI is accelerating both the volume and sensitivity of data in use, placing further pressure on environments that were never designed to operate as a single, governed system. Even where sovereign cloud strategies are in place, many enterprises are still working out how these environments fit together.

Documented intent rarely matches day-to-day handling. Enterprises need a clear, working view of how it is stored, replicated, processed and accessed across the full ecosystem.


The endpoint
is often known.
The path is
not.

Where is your traffic heading?

An organization may know where its cloud region is, yet have limited visibility into how traffic actually travels between environments, which networks it crosses and which jurisdictions it touches in transit.

Public IP networks were designed to prioritize efficiency, built for a different era of connectivity. Routing decisions are made dynamically, meaning data can pass through multiple providers and regions without predictability or control. From a sovereignty perspective, this creates a mismatch between dynamic routing and data sovereignty requirements.

Exposure increases here. Each additional network hop introduces more risk, more dependencies and more uncertainty over which legal regimes apply. Arelion's research reflects this clearly, with 83% of enterprise leaders agreeing that reducing third-party network hops improves data security.

As AI adoption accelerates, this becomes more pronounced. Data is moving continuously between environments as part of training, inference and real-time processing, and must meet regulatory scrutiny that changes by jurisdiction.

At the same time, evolving regulatory frameworks are creating an ever-changing compliance landscape, particularly in Europe, where national strategies must align with EU directives as well as global data sovereignty rules.

> Without visibility and control over how traffic moves across networks, enterprises cannot fully assess exposure or enforce sovereignty with confidence.

Proving control is where many organizations struggle

Businesses may define where data should reside, but demonstrating that consistently across complex, multi-provider environments is far more difficult. Arelion's research reflects this disconnect, with nearly half of organizations not fully confident they can demonstrate compliance to auditors.

The issue is rooted in how networks operate. IP packet technology is inherently route-agnostic, selecting paths based on efficiency. While the underlying infrastructure can be mapped, proving the exact path data takes is far from simple. Forcing traffic along specific paths is possible but introduces further complexity for traffic engineering teams already facing significant challenges.

This creates a gap between policy and evidence, where organizations prioritize sovereignty but struggle to operationalize it or define what "good" looks like.

Closing this gap requires a more operational approach. Enterprises must map data flows, document routing policies, maintain accurate asset inventories and rely on provider transparency and auditability to demonstrate control.

In 2026, sovereignty depends on provability – being able to evidence how data is managed, routed and protected across its full lifecycle.



AI introduces new value, but also new exposure



Enterprises are investing heavily in GPU clusters, data centers and AI platforms – often with a focus on compute capacity and model performance. The challenge emerges when connecting these environments to the wider enterprise ecosystem.

AI systems depend on continuous data exchange across cloud platforms, internal systems and external sources. In practice, this means connecting AI environments to core systems such as CRM, ERP, R&D and, in many cases, the public internet.

Without a clear approach, gaps begin to appear. Data flows become harder to track, dependencies increase, and exposure to multiple jurisdictions and third-party networks grows. What begins as a technical integration issue quickly becomes a performance and trust problem.

Governance is not keeping pace. According vto IBM, 63% of organizations lack formal AI governance policies[2], while 62% cite data sovereignty and privacy risks as the primary factor slowing AI projects in the public cloud, according to Arqit[3], with impacts on efficiency, competitiveness and customer experience.

AI value extends beyond raw compute. It depends on how effectively data can move across environments, and how consistently that movement is controlled and governed.

For enterprises, the question has shifted from, “How do we use AI?” to “How do we do so without creating unnecessary exposure?” AI assets only deliver value when they are usable, trusted and governable.

2 https://www.ibm.com/reports/data-breach
3 https://ir.arqit.uk/news-events/press-releases/detail/123/62-of-respondents-cite-data-sovereignty-and-privacy-risks-as-the-biggest-factor-slowing-ai-projects-in-the-public-cloud


Mitigating risk
in your network

Conclusions and recommendations

Enterprise leaders are under increasing pressure to rethink how data is managed across their networks. According to Gartner, over 75% of enterprises outside the US are projected to adopt formal data sovereignty strategies by 2030[4].

It is no longer a case of whether to act, but how quickly organizations can reorient and embed data sovereignty into how their environments are designed and connected. Those that get it right can create a more controlled and scalable foundation for how data is used. Those that don't risk creating unnecessary exposure.

There are a number of practical steps enterprises can take to reduce exposure and make sovereignty provable in practice.

[4] https://www.gartner.com/en/newsroom/press-releases/2025-11-12-gartner-survey-reveals-geopolitics-will-drive-61-percent-of-cios-and-information-technology-leaders-in-western-europe-to-increase-reliance-on-local-cloud-providers

Conclusions and recommendations

1.

Identify your AI ecosystem before designing for sovereignty

AI depends on a distributed ecosystem of applications, data sources and infrastructure working together. In many cases, the challenge is not the model itself, but how it connects across cloud platforms, internal systems and external services.

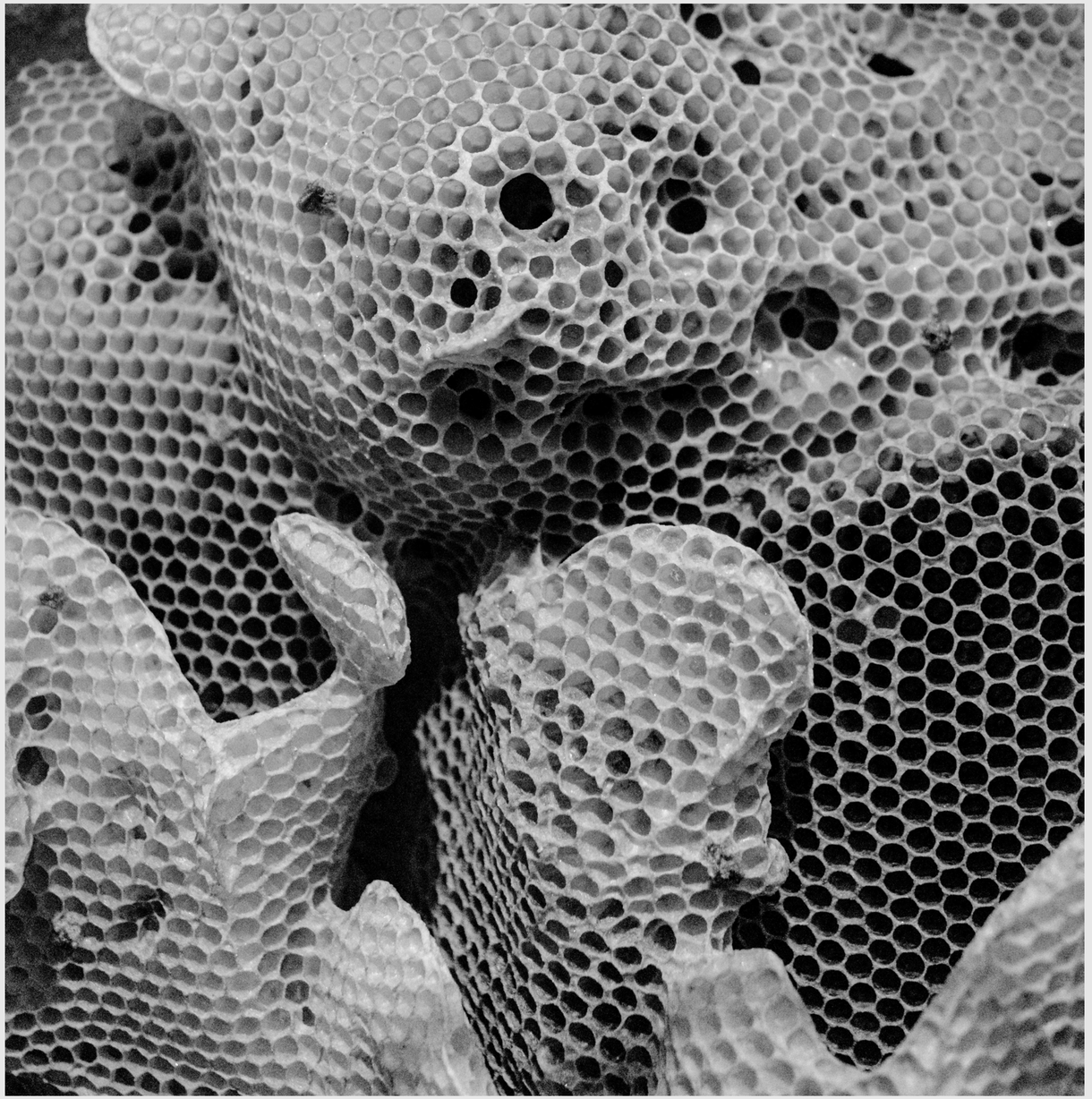
Start by mapping how these components interact, where data originates, and how it moves between environments. Without that visibility, sovereignty risks are introduced into the architecture from the outset.

2.

Align data criticality with risk tolerance

Not all data carries the same level of sensitivity, and not every AI use case requires the same level of control.

Assess both the criticality of the application and the sensitivity of the data it depends on, particularly as it flows across networks. Define acceptable levels of exposure in transit, especially where data crosses third-party environments. Sovereignty becomes more effective when it is aligned to business risk, rather than applied uniformly.



3.

Design for provability

Knowing where data is stored is not enough. Enterprises also need to understand how it moves between environments and which networks it traverses in transit.

Work with providers who can offer visibility into routing behaviour, minimize unnecessary intermediaries and validate how traffic enters and exits their networks. Without this, it becomes difficult to assess exposure or enforce policy.

4.

Scrutinize your providers and their supply chains

Data sovereignty extends beyond the provider itself to include ownership, operational control and the wider supply chain.

Assess who ultimately owns the provider, who operates your services and what their track record looks like. Clarify where services are delivered from, which entities are involved, and how responsibilities are structured across regions.

Review the provider's wider ecosystem. Identify which third parties they rely on, including cloud platforms, hardware vendors and network partners, where those suppliers are based, and what controls are in place to manage quality, security and compliance.

Select a provider that demonstrates strong network control and limits the number of third-party network hops, supporting industry and region-specific compliance requirements.

[4] https://www.gartner.com/en/newsroom/press-releases/2025-11-12-gartner-survey-reveals-geopolitics-will-drive-61-percent-of-cios-and-information-technology-leaders-in-western-europe-to-increase-reliance-on-local-cloud-providers

5.

Strengthen protection around exposed environments

As AI becomes more embedded in enterprise workflows, it increasingly relies on access to external systems, including SaaS platforms and public data sources. Agentic use cases in particular require continuous interaction beyond the corporate perimeter.

This expands the attack surface. Data is not only moving across more environments, but is also exposed to a broader threat landscape, where both geopolitical actors and criminal groups target critical services.

Assess how these connections are secured and controlled in transit, including how directly traffic is routed and whether exposure to third-party networks can be reduced. Consider the diversity and redundancy of the provider's network, and how it performs under disruption.



Arelion helps enterprises navigate data sovereignty challenges

The challenges in this guide reflect a consistent issue: how little control enterprises have once data leaves the corporate perimeter.

That is where Arelion plays a central role.

Arelion provides the network layer that connects cloud platforms, data centers and global infrastructure. Built on the world's #1 ranked IP backbone and a unique ecosystem of cloud and network service providers, it enables enterprises to move data more directly between environments, reducing reliance on unpredictable public internet paths.

This more controlled approach to routing limits unnecessary third-party dependencies, giving enterprises clearer insight into traffic flows and reducing exposure to unknown jurisdictions.

With improved visibility into how traffic is handled in transit, enterprises are better positioned to meet regulatory expectations, respond to audit requirements and make more confident decisions about risk across complex environments.

As data volumes grow and AI adoption accelerates, the pressure on enterprise networks will continue to mount. In this environment, the ability to understand and control how data moves is becoming a defining factor in how organisations operate.

Those that can establish that level of control will be well placed to navigate what comes next. Those that do not will face higher exposure as complexity grows and scrutiny intensifies.



Arelion

Next steps

—

Read the guide —

How to design for data sovereignty

A practical guide to building visibility, control, and provability into enterprise connectivity.

Download here →

Download full data protection report —

Connecting through chaos

This new report reveals where organizations are struggling, where risks are growing, and what leaders are doing to stay ahead.

Download here →