

Avoiding digital sovereignty tradeoffs

Incorporating sovereignty into IT and security purchasing decisions without compromising on functionality or resilience



Governments and companies around the world are increasingly concerned about dependency on foreign technology service providers. Unfortunately, moving large portions of the IT and security stack to 'sovereign' local providers can impede the same resilience and security such moves mean to protect.



33%

quarter-over-quarter increase in hyperscale DDoS attacks through 2025 — a challenge for many region-specific security providers¹



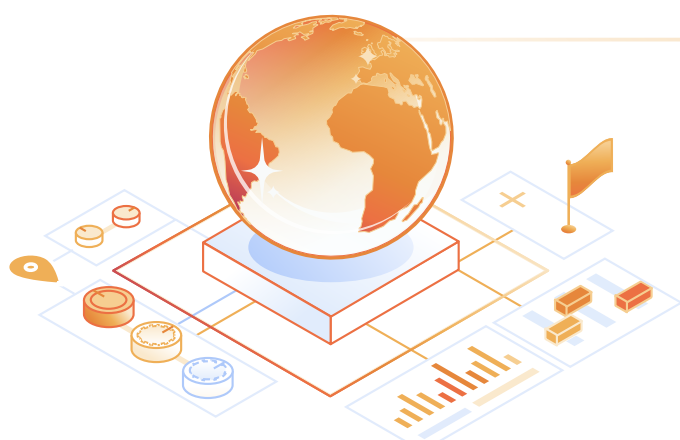
200%

projected increase in technology integration costs as organizations split AI stacks across sovereign zones²

These four strategies can help organizations avoid tough tradeoffs between sovereignty and security

1. Define and prioritize specific sovereignty risks

Getting specific about sovereignty needs across different security and IT practice areas helps you avoid unnecessary tradeoffs.

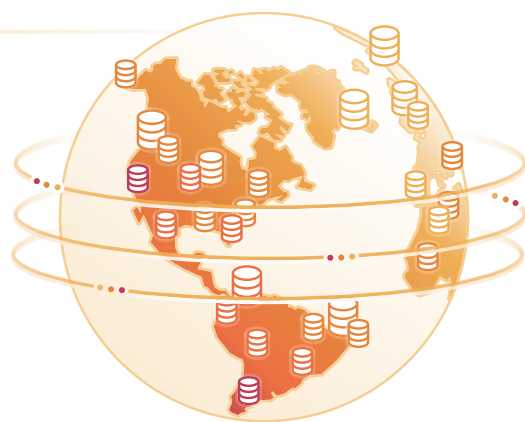


2. Explore programmability and customizability options

Will providers let you run some services globally, while still controlling where data is decrypted and inspected, who can access keys, where logs are stored, and more?

3. Consider multi-provider and failover compatibility

How easy do global providers make it to back up data, run alongside local secondaries, and implement failover strategies?



4. Investigate vendors' sovereignty governance policies

How transparent are providers about prior government requests? What is their policy for handling those requests?

See how these strategies led organizations like Doctolib and the Republic of Estonia to Cloudflare.

Learn more about Cloudflare's sovereignty approach



© 2026 Cloudflare, Inc. All rights reserved.
CLOUDFLARE® and the Cloudflare logo are trademarks of Cloudflare. All other company and product names and logos may be trademarks of the respective companies with which they are associated.

1 888 99 FLARE | enterprise@cloudflare.com | [Cloudflare.com](https://cloudflare.com)
REV:BDES-XXXX.2026APR15

Sources:

- <https://blog.cloudflare.com/ddos-threat-report-2025-q4/>
- <https://www.idc.com/resource-center/blog/the-high-cost-of-sovereignty-in-the-age-of-ai>