The shift to sovereignty in global governments

A new survival strategy for public sector organizations

For public sector organizations outside the United States, digital sovereignty has expanded from a regulatory checklist into a survival strategy. Governments now realize that sovereignty or compliance with jurisdictional laws alone is insufficient. The new digital sovereignty objective is referred to as strategic autonomy: the ability to operate, innovate, and maintain critical services independently, even when external support is withdrawn or global supply chains are disrupted.

A recent UN Trade and Development (UNCTAD) report stated, "79% of countries with legislation in privacy and data protection are concerned about digital sovereignty."[1] Governments can no longer afford to ignore the dependencies inherent in closed, proprietary systems. Transforming to strategic autonomy is influenced by 3 factors:

- **Geopolitical risk:** In peacetime, reliance on global hyperscalers is manageable. However, in conflict scenarios, reliance on external support becomes a critical vulnerability. Physical destruction or internet outages cripple cloud-dependent operations. Nations must possess the capacity to act independently when international cooperation is impossible or unreliable. This action requires systems capable of operating in denied, disrupted, intermittent, and limited (DDIL) environments, ensuring functions that are critical to the mission—from defense command-and-control systems to emergency citizen services—remain operational even if the country is disconnected from the global internet.
- **Cyber resilience:** State-sponsored cyberattacks are growing in sophistication, frequency, and influence. Sovereignty assures that critical infrastructure, such as energy grids, healthcare systems, and defense system networks, remains resilient against external interference and supply-chain sabotage. The risk includes data theft, but also the insertion of malicious code into software updates in transit. Governments require assurance of sovereignty: the ability to independently verify the integrity of their software supply chain to prevent foreign espionage, and that systems have not been compromised.
- **Economic competitiveness:** Governments increasingly view digital sovereignty as a cornerstone of national security. By localizing AI development and data governance, engines of future economic growth remain under domestic jurisdiction rather than external oversight. There is a growing concern that relying on foreign black-box AI models will lead to a loss of intellectual property and cultural relevance. Strategic autonomy allows nations to build these digital capabilities, fostering local innovation ecosystems and ensuring that the economic value generated by their digital transformation remains within the national economy.

1 "Data protection and privacy legislation worldwide." UNCTAD, 17 Feb. 2026.

Global demand, regional realities

While the demand for control is global, the specific influences and barriers faced by the global public sector vary significantly by region.

Europe, Middle East, Africa and Canada (EMEA)

The primary friction in EMEA is the tension between the need for advanced technology and the reliance on non-European Union (EU) providers, which exposes governments to jurisdictional risk, specifically extraterritorial laws like ones enacted by the United States, including the Clarifying Lawful Overseas Use of Data (CLOUD) Act or the Foreign Intelligence Surveillance Act of 1978 (FISA).

European agencies face a complex web of stringent regulations, including the EU's NIS2 for cybersecurity and Digital Operational Resilience Act (DORA) for operational resilience, alongside national mandates like France's SecNumCloud. Defense infrastructure remains fragmented, with North Atlantic Treaty Organization (NATO) interoperability gaps delaying data exchange. Additionally, countries face critical shortages of security-cleared staff to operate sovereign environments. Though geographically in North America, Canada shares EMEA's challenges regarding outdated infrastructure. Canada's Department of National Defence struggles with a fragmented patchwork of Consolidated Secret Network Infrastructure (CSNI) and bureaucratic hurdles that slow the adoption of modern capabilities. The level of risk causes government agencies to insulate sensitive data from foreign legal interference and closes the software gap by building homegrown capacity.

Asia Pacific (APAC)

The APAC region is defined by strict protectionist mandates and high-stakes compliance to achieve technological self-reliance.

- **Data localization:** Nations such as China, India, and Indonesia enforce strict data localization, requiring critical data to reside entirely within national borders, limiting the use of global public clouds.
- **High accountability:** Singapore imposes rigorous end-to-end security standards, under which public officers can face criminal penalties for data misuse or misplacement, prompting a risk-averse procurement culture.
- **Global and local requirements:** There is a strong preference for global and local models (glocal)—partnerships in which global tech is delivered via local firms to ensure there is sovereign control.

A focus of the APAC nations is to develop native capabilities to reduce long-term dependence on foreign powers, viewing digital sovereignty as a shield against geopolitical vulnerability.

Latin America (LATAM)

Modernization in LATAM is influenced by operational continuity and is often hindered by structural instability rather than policy.

- **Instability and discontinuity:** Frequent changes in political leadership and economic volatility jeopardize long-term IT planning and multiyear procurement contracts in an uncertain geopolitical climate.

- **Internal security focus:** LATAM defense agencies prioritize internal security (border protection, counter-narcotics), favoring agile surveillance tools rather than heavy strategic infrastructure.[2]
- **Procurement risks:** Inefficiencies and corruption risks in public procurement reduce the effective value of technology budgets, prompting a need for cost-effective, open, and flexible systems that can survive budget cuts and political shifts without locking the nation into expensive, rigid proprietary vendors.

A Red Hat approach to digital sovereignty

To succeed, global public sector agencies must address sovereignty across these distinct dimensions. Red Hat provides the tools and ecosystem to comprehend each.

Data sovereignty and AI

Red Hat understands the criteria of full control and autonomy over critical data and AI models, ensuring data residency within national borders and governance that aligns with local laws. Agencies must implement sovereign AI strategies that retain ownership of their models and training data, deploying them on localized infrastructure rather than relying on application programming interface (API) access to foreign-controlled models. Red Hat® OpenShift® AI allows the deployment of sovereign AI capabilities where the data resides. We empower control over data location and access by using confidential computing to protect data in use, ensuring compliance with regulations like the EU AI Act.

Technology sovereignty

The ability to run workloads without depending on a specific provider's infrastructure or proprietary software is required to ensure long-term independence and the ability to move applications without restrictions. Governments should avoid vendor lock-in by adopting open standards and portable container platforms. If a cloud provider's policies change or geopolitical tensions rise, workloads can be migrated to another infrastructure without refactoring. Red Hat reduces vendor lock-in through open source standards. Our platform supports multiple hardware architectures (x86, Advanced RISC Machine (ARM), RISC-V), so that national systems can evolve and update on their own schedule, independent of external dependencies.

Operational sovereignty

Government agencies need to maintain full administrative authority and independence over their critical IT operations to survive and operate even when disconnected. Defense and critical infrastructure must prioritize operational resilience. This infrastructure involves automating disaster recovery plans that account for wartime conditions and ensuring that support and operations are managed by local, security-cleared citizens. For example, Red Hat offers confirmed sovereign support, technical support that is provided by verified local citizens (e.g., within the EU), ensuring no data accessible by support staff leaves the jurisdiction. Additionally, Red Hat Ansible® Automation Platform automates resilience, providing rapid recovery and patching even in disconnected (DDIL) environments.

Assurance sovereignty

Independently verifying the integrity, security, and reliability of digital systems and processes helps agencies remain compliant. Agencies must move from blind trust to verifiable trust. This move requires rigorous auditing of the software supply chain and the ability to demonstrate compliance with standards

2 "New Pentagon strategy to focus on homeland, Western Hemisphere." DefenseNews, 25 Sept. 2025.

such as Common Criteria, Federal Information Processing Standards (FIPS), and NIS2. Red Hat provides a trusted software supply chain, delivering cryptographically signed software with verified provenance and a software bill of materials (SBOM), allowing agencies to audit every component and ensure no malicious code has been injected. These safety measures help make certain that agencies are meeting emerging mandates like the EU Cyber Resilience Act.

Strategic autonomy through open source

Red Hat uses a flexible, open foundation to address challenges, granting government agencies more choice and control instead of rigid isolation. This flexible approach acknowledges that a single provider rarely solves digital sovereignty. Red Hat offers the choice to build a sovereign cloud across various infrastructure providers and cloud zones, avoiding the limitations of a single solution.

For more than 30 years, Red Hat has delivered trusted, enterprise open source solutions to organizations with the most stringent security and compliance requirements. Enterprise open source is not merely a technology, but an essential architectural foundation for government agencies to see true digital sovereignty and strategic autonomy. Unlike proprietary vendors that rely on closed, opaque systems and require blind trust, Red Hat helps agencies maintain absolute control over their digital destiny rather than relying on others. This open approach helps the global public sector to control the speed of global innovation—from the tactical edge of the network to sovereign AI—while ensuring workloads remain portable and resilient. An open source approach also safeguards mission-critical operations from the risks of vendor lock-in and technological obsolescence. By using open source technology, Red Hat aligns with a default to open doctrine prevalent in regions like the EU. Using a model like this prevents dependence on a single vendor and allows code inspection and modification, becoming essential for national security and trust.

- **Transparency and trust**

  Red Hat's open source model offers 100% transparency, allowing government agencies to inspect the source code, verify security, and audit software supply chains. This auditability is critical for meeting assurance requirements in EMEA and APAC. Furthermore, Red Hat delivers cryptographically signed software with verified provenance to meet emerging mandates, such as the EU Cyber Resilience Act.

- **Operation sovereignty and local support**

  To address jurisdictional risks, Red Hat supports the ability to control who operates the infrastructure to achieve operational sovereignty.

  - **Sovereign support:** As mentioned previously, Red Hat offers confirmed sovereign support in the EU, making certain that technical support is provided exclusively by verified EU citizens located within the EU. This technical support helps ensure that no data accessible by support staff leaves the region.

  - **Local ecosystems:** An ecosystem of Red Hat partners with local, certified cloud providers is available to deliver sovereign cloud capabilities that meet strict national residency laws.

- **Technological independence**

  An open hybrid cloud strategy allows workloads to run in many environments, such as on-premise, in a private cloud, at the tactical network edge, or in an air-gapped environment.

- **Portability:** This is the foundation for preventing vendor lock-in, a paramount concern for government agencies, particularly in regions like LATAM and APAC. The ability of these regions to efficiently migrate workloads and data is a critical requirement to ensure service continuity and efficient responsiveness to geopolitical changes, such as political or economic shifts that may necessitate switching technology providers.
- **Disconnected operations:** For defense agencies, Red Hat solutions such as Red Hat Device Edge and Red Hat OpenShift allow systems to function autonomously in disconnected DDIL environments, ensuring mission survival even if a central cloud is unreachable.

Red Hat gives government agencies the open foundation to build a sovereign cloud that survives uncertainty, offers reliable data security, and keeps the nation running.

- **Sovereign AI**

  As governments explore and expand AI, Red Hat provides the platform to build sovereign AI. This helps make sure nations retain ownership of their models and training data, deploying them on localized infrastructure to comply with regulations like the EU AI Act, rather than relying on API access to foreign-controlled models.

Why Red Hat for the public sector?

Red Hat has been a trusted partner to the public sector, deployed in 100% of U.S. executive departments[3] and widely used across NATO and global ministries of defense. A Red Hat licensing model and commitment to open standards ensure that agencies are never coupled to a vendor in perpetuity. Organizations retain the right to use and maintain software indefinitely, protecting long-term investments against shifting vendor roadmaps or geopolitical restrictions.

As spending increases, particularly in the defense sector, an investment in Red Hat's portfolio of solutions and services can show a visible return on investment. Member nations' spending commitments to NATO will double, reaching 5% of national GDP by 2035.[4] By standardizing on a unified platform, agencies can shift investment from maintaining fragmented conventional systems to generating new mission capabilities, significantly reducing operational costs and total cost of ownership.

Next steps to get started

- Learn more about Red Hat in the global public sector and talk to a Red Hatter.
- Interested in assessing your digital sovereignty readiness? Read this blog post to get started.

3 Red Hat client data, Sep. 2025.

4 "Defence expenditures and NATO's 5% commitment." NATO, 18 Dec. 2025.

facebook.com/redhat
x.com/RedHat
linkedin.com/company/red-hat

redhat.com
#3613114_0326

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com