Red Hat Summit

Connect

Take back control – How open source can strengthen your Digital Sovereignty

Monica Sasso

Red Hat
Global financial services digital transformation lead

What we'll discuss today

- What is digital sovereignty

  Interplay with operational resilience

- Why is digital sovereignty a dinner party discussion now?

  Context, interplay with operational resilience

- How Red Hat supports its clients' digital sovereignty goals

  Open source software, our commitment, sovereign cloud enablers

What is digital sovereignty?

- What does digital sovereignty mean
- What does it mean as we move towards an AI centric world?
- Cloud adoption models

Cloud usage & digital transformation have been reshaped by regulatory requirements in the financial services & insurance industries

2018+

Data Privacy: GDPR, Schrems II, LGDP, PIPEDA, PIPL, etc

2025

DORA, Operational Resilience, NIS 2, etc

2025+

Directive on

(CIR)

2026+

Cloud / Digital sovereignty, EU AI Act

https://www.whitecase.com/insight-our-thinking/financial-regulatory-observer-2022-operational-resilience-uk-eu-and-us

Digital sovereignty refers to the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create.

Or, as the Centre for Africa-Europe Relations puts it: the physical layer (infrastructure, technology), the code layer (standards, rules and design) and the data layer (ownership, flows and use).

Source: "What is digital sovereignty and why is Europe so interested in it?" (Sean Fleming, World Economic Forum, March 15, 2021)

Dimensions of digital sovereignty

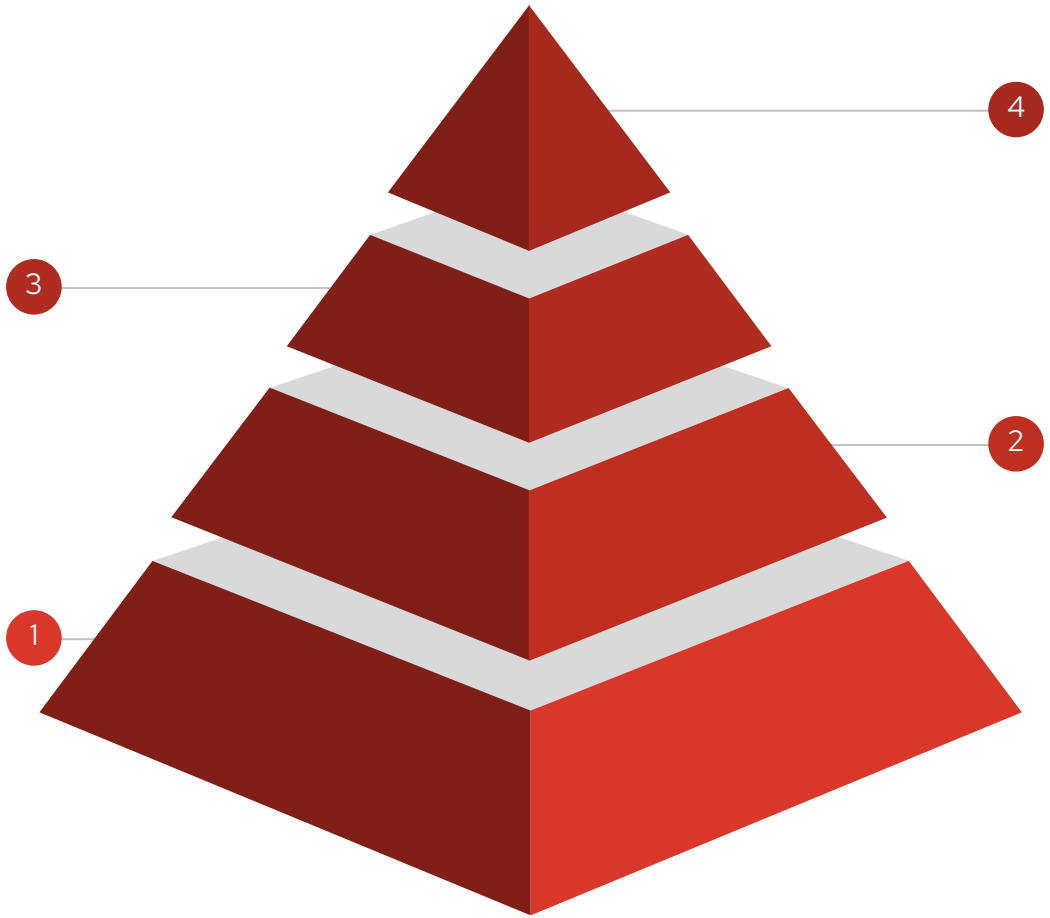
Similar to operational resilience, it is a continuum, reflecting a range of practices and policies that nations legislate to manage and control their digital assets, data and technology infrastructure

Operational Sovereignty

Visibility and control over provider operations from provisioning and performance management, to monitoring of physical and digital access, to the infrastructure.

Data Sovereignty

Maintaining control over how data is collected, classified, processed and stored to ensure that data regulations are met



Assurance Sovereignty

Ability to independently verify and assure the integrity, security, and reliability of digital systems and processes, including resilience of critical services.

Technical Sovereignty

Running workloads without dependence on a provider's infrastructure or software, and protected from all extraterritorial interference and scrutiny.

Sources:

"Sovereign Clouds and the Digital Sovereignty Imperative: Europe's Quest for Digital Independence" (IDC #EUR149098122, December 2022)

The Evolution of Digital Sovereignty: Moving Beyond Data and Cloud" (Rahiel Nasir, IDC, January 13, 2023)

The reality of digital sovereignty

Various stakeholder groups see digital sovereignty through different lenses

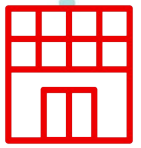
Governments & nation states

- National security
- Reducing extraterritorial reach
- Cybersecurity & protecting critical national infrastructure
- Supply chain risk
- Preventing digital interference
- Citizens' rights
- Protecting their local economies

Citizens (so US!)

- Data privacy & control over our data
- Choice
- Safeguarding democracy, autonomy & national resilience
- Fostering a local digital economy
- Culture

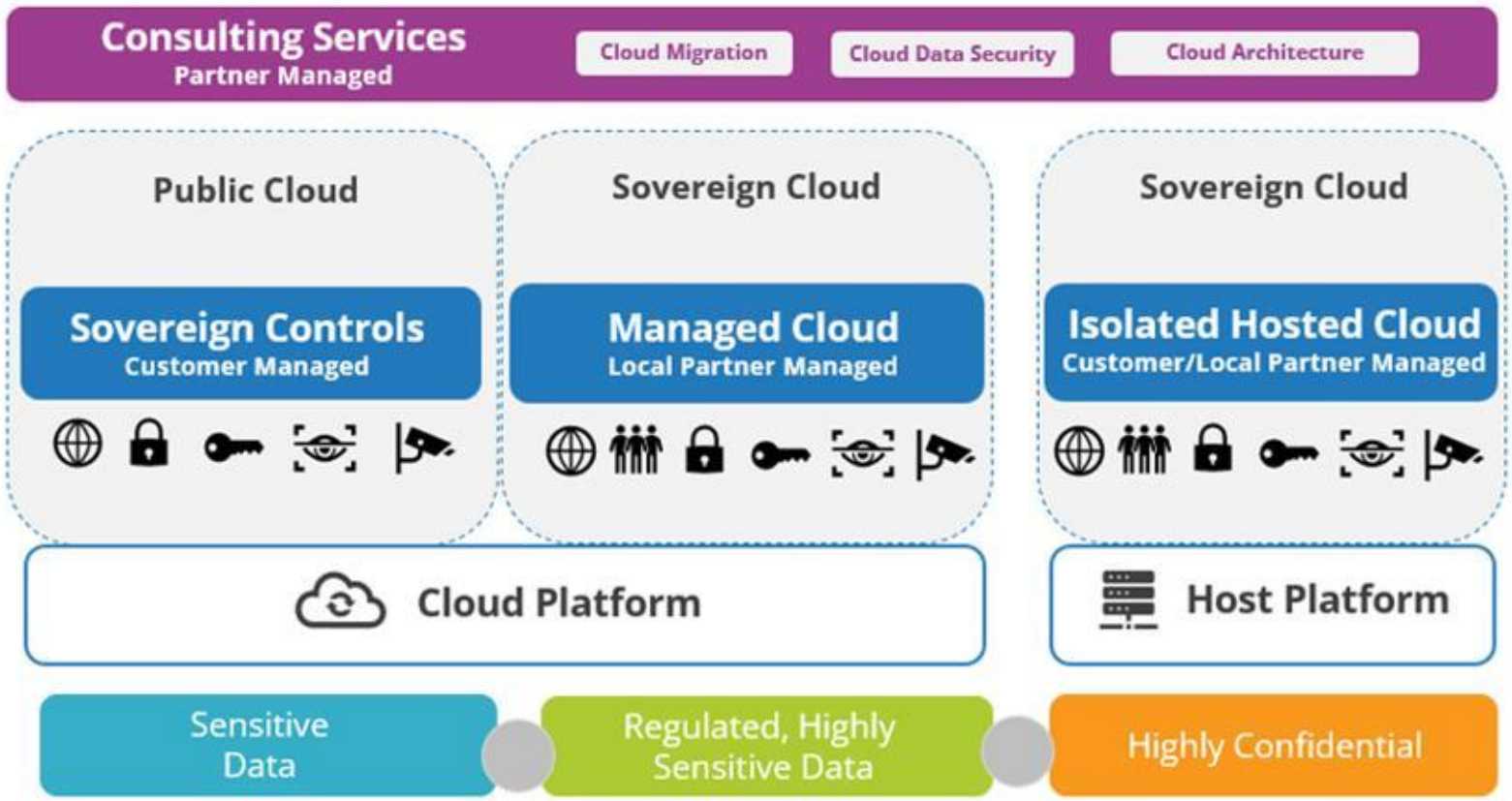
Businesses (the economy)



- Protecting IP
- Fair competition
- Business continuity
- Operational resilience
- Compliance in a modern data-driven world.
- Concentration risk (of 3rd party providers
- Domestic talent
- Strategy . . .

Sovereign cloud adoption models

82% of firms in Europe are either currently or planning to use sovereign cloud solutions offering varying degrees of control, security and local compliance in coming years



Sovereign Controls: Built-in platform controls offered by the public cloud provider, which the customer manages. These controls include data residency, encryption/key management, and access management.

Managed Cloud: The cloud provider collaborates with a local trusted partner who independently administers the sovereign controls and provides strict local control over deployments and operational access.

Isolated Hosted Cloud: Dedicated (private) cloud service delivered natively from sovereign cloud datacenters by partners.

Sources:

"Digital Sovereignty: Building Greater Security, Trust, and Business Resilience in Europe" (Rahiel Nassir, IDC)

"IDC's Worldwide Digital Sovereignty Taxonomy, 2023: Cloud Sovereignty"

Why is digital sovereignty a dinner party discussion now?

- Context
- Digital sovereignty & AI adoption

Why now?

Resilience bleeding into sovereignty: configuration errors happen

Google accidentally deletes pension fund from its cloud platform


Leadership

Google praises UniSuper's CIO after GCP error deleted $124 billion firm's entire private cloud

Post-mortem praises Aussie fund's good third-party backups, "speed and precision" from CIO's team

The Stack
May 27, 2024 - 2 min read

More than half a million UniSuper fund members went a week with no access to their superannuation accounts

- Duplication in two geos didn't help, because the whole GCP subscription was deleted
- Deletion grace period was also misconfigured

UniSuper was able to eventually restore because they had **backups with another provider**

https://www.thestack.technology/google-praises-unisupers-cio-after-it-deleted-124-billion-firms-private-cloud/

Why now?

Geopolitics bleeding into tech: immediate service denial

Sanctions made it impossible for Microsoft to discontinue providing O365 to the ICC's chief prosecutor

Exclusive: US could hit entire International Criminal Court with sanctions soon

By **Anthony Deutsch, Humeyra Pamuk** and **Stephanie van den Berg**

September 23, 2025 4:45 PM GMT+1 · Updated September 23, 2025

British ICC chief prosecutor lost access to email and has bank accounts frozen after Trump sanctions on top court

- Chief prosecutor of the International Criminal Court, Karim Khan, lost access to his (Microsoft) email when Donald Trump imposed sanctions on him in February 2025 in response to the ICC issuing arrest warrants for Israeli prime minister Benjamin Netanyahu and his former defence minister Yoav Gallant in November.
- Khan's bank accounts in Great Britain were also frozen

https://www.lbc.co.uk/article/british-icc-chief-prosecutor-lost-email-bank-accounts-frozen-trump-sanctions-rpTkm_2/
https://www.reuters.com/world/europe/us-could-hit-entire-international-criminal-court-with-sanctions-soon-2025-09-22/

Example

Cybercrime reducing resilience: back-doored critical infrastructure

Rogue communication devices found in Chinese solar inverters and batteries

- “China Holds a Kill Switch to **European** Power Grids”
- “**US** energy sector at risk, as Chinese inverters are under investigation for suspicious communication gear”
- “Estonia's Director General of the Foreign Intelligence Service, Kaupo Rosin, said the country could be at risk of blackmail from China if it did not ban Chinese technology in crucial parts of the economy, such as solar inverters.”

https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
https://industrialcyber.co/utilities-energy-power-water-waste/us-energy-sector-at-risk-as-chinese-inverters-are-under-investigation-for-suspicious-communication-gear/
https://chinaobservers.eu/china-holds-a-kill-switch-to-european-power-grids/

Smart tech compromising food supplies

What John Deere did to Russian looters, anyone can do to farmers, anywhere.

Remote bricking of Ukrainian tractors raised agriculture security concerns

- Modern tractors are intelligent machines
- Hackable tractors are vulnerable to sabotage
- Tractor VIN-locks (forcing farmers to be locked in to using authorised dealers for repairs) fueled the “right to repair” movement

https://www.csoonline.com/article/572811/remote-bricking-of-ukrainian-tractors-raises-agriculture-security-concerns.html

. . . . leading to . . . .

Geopolitics shaping modern technology & AI adoption

- AI adoption is fragmented and based on nation-states' needs: i.e. medical, agricultural vs efficiency and cost savings

- Defined by three main approaches:
  - Regulatory led
  - State-Led
  - Swing States

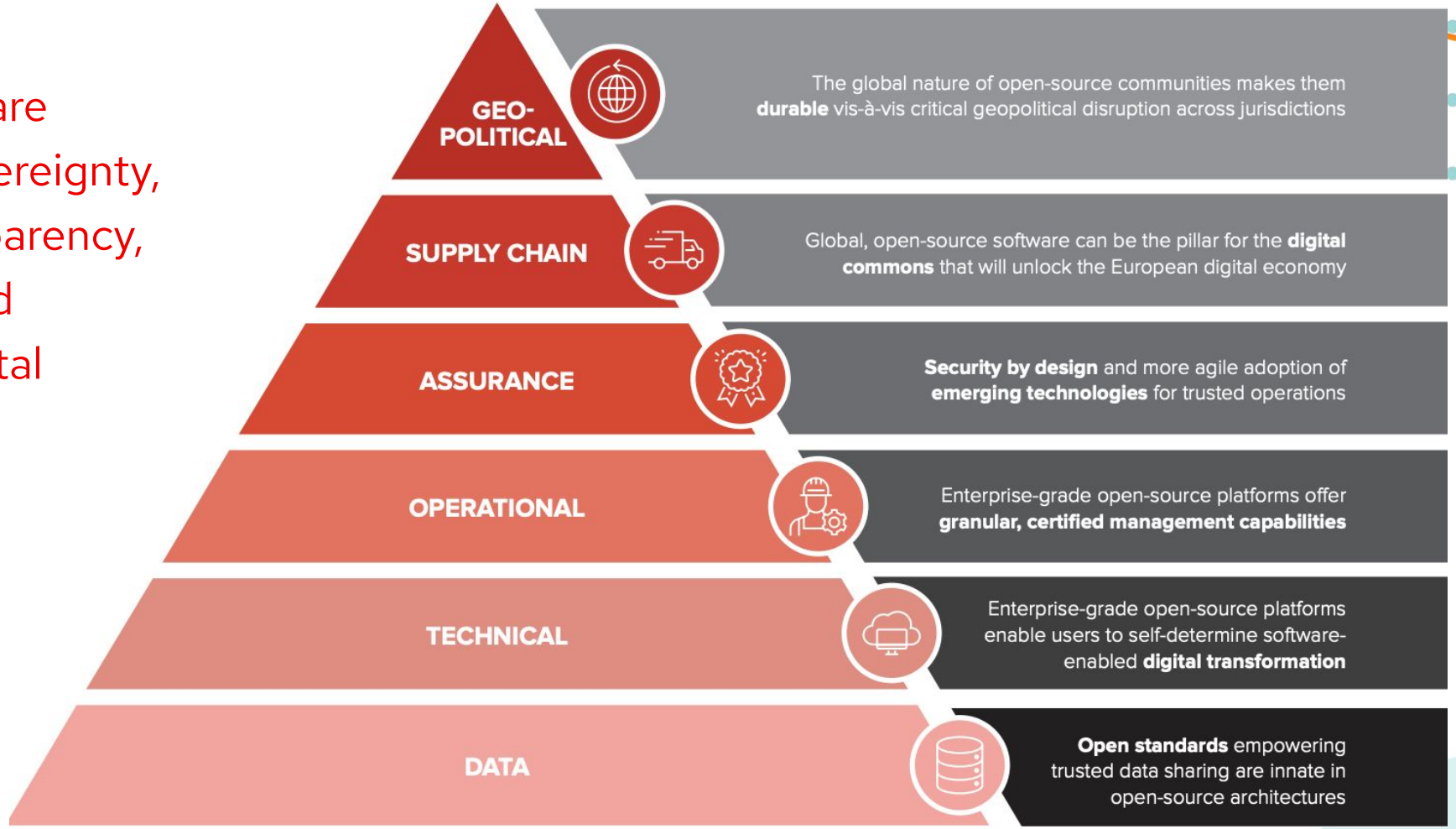
In confusing and uncertain times, planning for options (and failure)is crucial to keeping your business up and running

How Red Hat supports its clients' digital sovereignty goals

- Open source software
- Digital sovereignty from a platform company's view
- Digital sovereignty technology enablers: confidential compute & everything as code
- Our commitment

Open Source as an accelerator to digital sovereignty

Open Source software supports digital sovereignty, by promoting transparency, control, security, and resilience in the digital landscape



Sources:

"Open Source and Digital Sovereignty: Two Sides of the Same Coin" (IDC #EUR20220729, October 2022)

A tech firm's vision of the open hybrid sovereign cloud

Underpinned by the cloud reversibility principle and modern platform best practices

Yesterday	Today	Future
On-premise Datacentre	On-premise and Public Clouds	IT environment extends to distributed edge
Datacentre centric IT	**Multi & Hybrid Cloud Adoption**	**Workloads on Edge**
Trusted Open Source Software	**Multi-Cloud GitOps Patterns for XaaS**	**Data Federation**

Cloud reversibility principle supported by capabilities for technical, operational and data sovereignty

Extending traditional thought leadership on open standards and interoperability beyond technology to include operations and data

Cloud reversibility in practice: avoiding operational lock in

A cloud-native, cloud-agnostic deployment approach via a continuous IT stack gives true control, choice and autonomy over systems and data

Data Layer

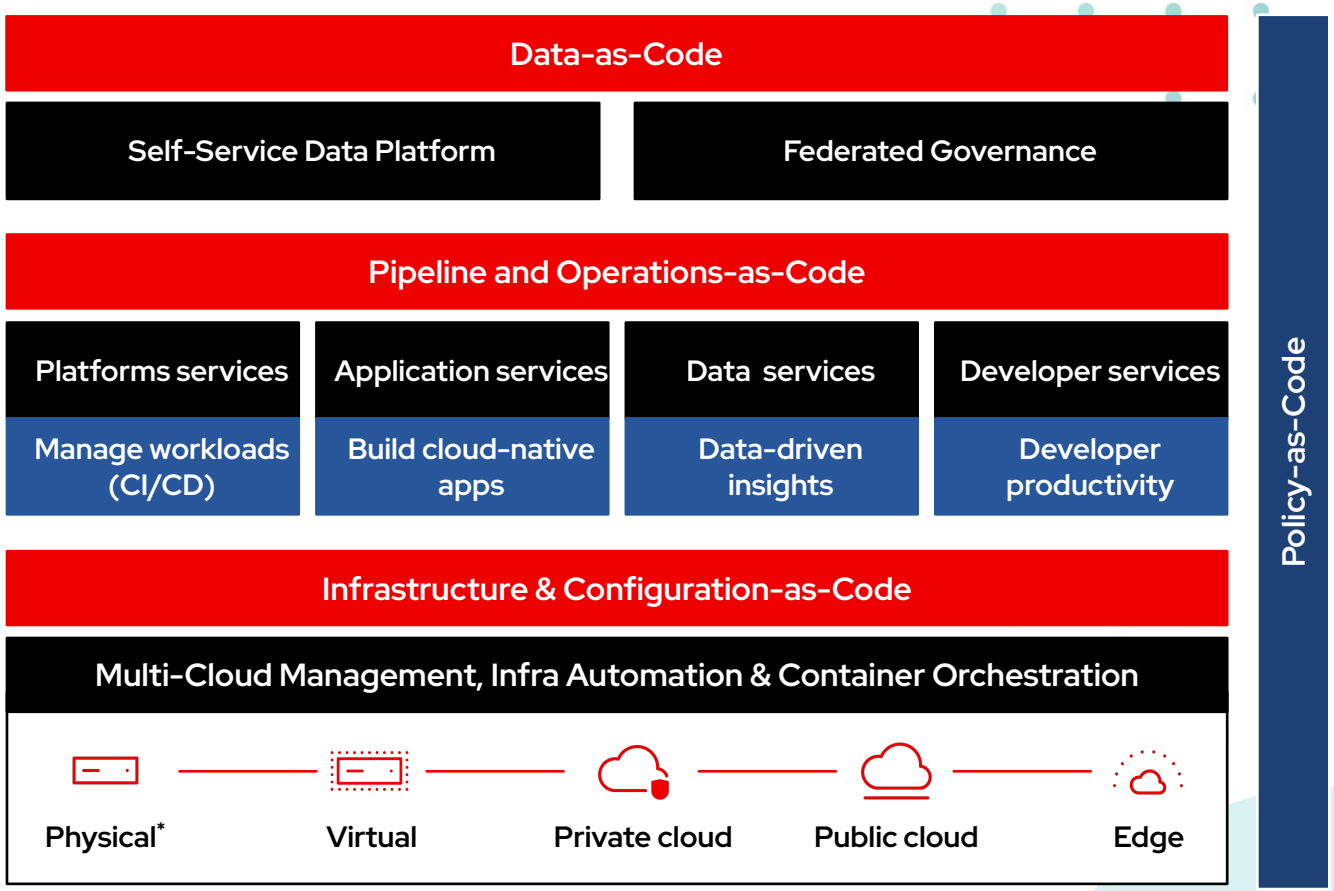
Allows the firm to keep control of its data in the cloud, prevent unsolicited third-party access and maintain regulatory rules for data at rest and in transit.

Operational Layer

Gives firms visibility and control of its operations while maintaining continuity of operations and regulatory compliance.

Technical Layer

Gives firms the ability to run workloads without continuous dependence on a specific provider's cloud infrastructure, software or services.



Red Hat's approach to digital sovereignty

Our 5 core commitments

1. **Transparency and Trust** with open source software.
2. **Control and Choice** with a flexible open hybrid cloud approach.
3. Robust Protection, **Operational Resilience** and Stability of critical infrastructure.
4. Building and Collaborating with a **strong ecosystem of local partners**.
5. Unlocking the **Future** of Sovereign AI Workloads.

https://www.redhat.com/en/blog/red-hats-commitments-sovereign

Red Hat Summit

Connect

Thank you


linkedin.com/company/red-hat


facebook.com/redhatinc


youtube.com/user/RedHatVideos


twitter.com/RedHat