VMware Sovereign Cloud Solution Overview

Composition and benefits

"Data is the new oil."

CLIVE HUMBY
BRITISH MATHEMATICIAN
AND DATA SCIENTIST

DEFINITION OF TERMS

- **Sovereignty** is the power of a state to do everything necessary to govern itself, such as making, executing, and applying laws; imposing and collecting taxes; making war and peace; and forming treaties or engaging in commerce with foreign nations.

- **Data residency** is the physical and geographic location where data is stored and processed.

- **Data sovereignty** refers to data being subject to the privacy laws and governance structures within the nation where data is collected.

- **Jurisdiction** is the limit of a legal authority. It can refer to political territories, geographic regions, and or the types of legal matters over which a legal body has authority.

The emergence of sovereign cloud

The concept of sovereignty is emerging as a necessary component of cloud computing for many entities that process and maintain highly sensitive data, such as national and state governments, and highly regulated industries, such finance and healthcare. National governments are also looking to expand digital economic capability and reduce reliance on multi-national firms for their cloud services.

VMware defines a sovereign cloud as one that:

- Protects and unlocks the value of critical data (e.g., national data, corporate data, and personal data) for both private and public sector organizations
- Delivers a national capability for the digital economy
- Secures data with audited security controls
- Ensures compliance with data privacy laws
- Improves control of data by providing both data residency and data sovereignty with full jurisdictional control

While keeping data 'in' is a key concern for sovereignty, it is also necessary to securely share data outside of its jurisdiction when warranted. For example, cross-border policing activities and collaboration. The secure sharing and monetization of data across borders is very important as we look to the next generation of currency - data.
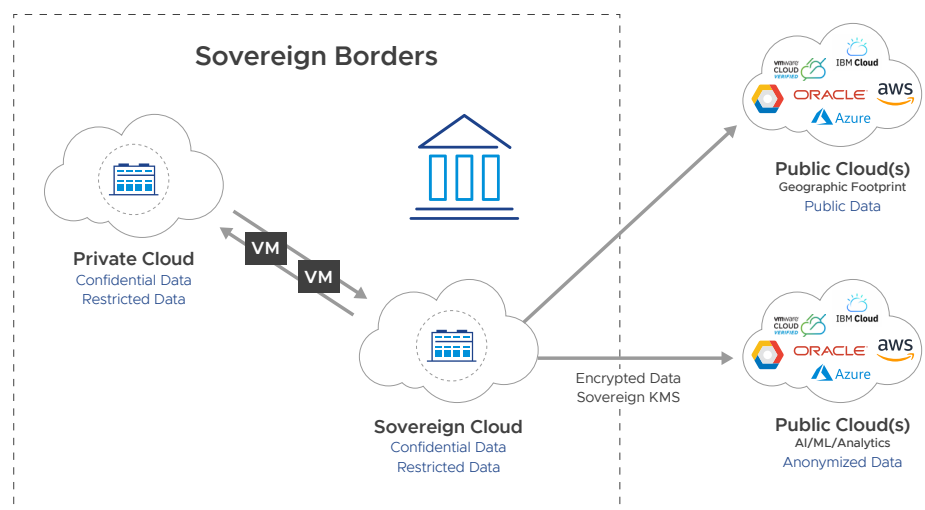

FIGURE 1: Sovereign clouds augment hyperscale public clouds by leveraging shared data across borders

SUMMARY OF VMWARE SOVEREIGN CLOUD FRAMEWORK PRINCIPLES

- **Data Sovereignty and Jurisdictional Control** – All data is resident and subject to the exclusive control and authority of the nation state where that data was collected. Operations are fully managed within the jurisdiction.

- **Data Access and Integrity** – Cloud infrastructure is resilient and available in at least two data center locations within the jurisdiction with secure and private connectivity options available.

- **Data Security and Compliance** – Information security management system controls are certified against an industry recognized global (or regional) standard and audited regularly.

- **Data Independence and Mobility** – Support for modern application architectures to prevent vendor cloud lock-in and enable application portability and independence.

LEARN MORE

To learn more about VMware Sovereign Cloud, please visit www.cloudsolutions.vmware.com/services/sovereign-cloud.

To connect with a VMware Cloud Provider in your region, please visit www.cloud.vmware.com/providers/sovereign-cloud or contact your VMware representative.

Partnering with a trusted sovereign cloud service provider

To ensure success, organizations must work with partners they trust and that are capable of hosting authentic and autonomous sovereign cloud platforms. VMware Cloud Providers recognized within the VMware Sovereign Cloud initiative commit to designing and operating cloud solutions based on modern, software-defined architectures that embody key principles and best practices outlined in the VMware Sovereign Cloud framework.

VMware Sovereign Cloud framework principles

Data Sovereignty and Jurisdictional Control | Data Access and Integrity | Data Security and Compliance | Data Independence and Mobility

VMware Cloud Providers abiding by the VMware Sovereign Cloud framework deliver added value by helping their customers to:

Increase Security
- Implement security controls in the cloud more quickly and effectively
- Secure data and workloads against rapidly changing attack vectors

Maintain Compliance
- Achieve compliance significantly faster and more efficiently
- Demonstrate compliance on an ongoing basis, rather than every few months

Improve Control
- Ensure visibility and auditing of all cloud administration and activities
- Prevent unauthorized or authorized access to data by foreign entities

Unlock Data
- Share and extend data with trusted nation states, companies, or clouds
- Leverage advanced services to enable data insights and ensure data integrity

Future Proof
- Avoid vendor lock-in
- Against changing regulations, security threats and geopolitics

Fuel Economic Innovation
- Develop a national and sovereign digital capability
- Pool national data to unlock economic innovation and growth