Return of Sovereign Cloud
Part 1: Commercial
Value Proposition
Protecting and unlocking the value of critical data

Co-authors:
Patrick Verhoeven, Cloud Strategist, VMware Multi-Cloud Strategy and Architecture
Stuart Lee, VMware Chief Data Privacy Officer
# Table of contents

- Introduction ......................................................... 3
- Emergence of data privacy regulations .............................. 3
- Data privacy is not getting easier ................................... 4
- Growing need for Sovereign Clouds ................................. 5
  - Ensure data privacy ........................................... 5
  - Fuel innovation and economic growth .......................... 5
- Data residency and data sovereignty ................................ 6
  - Data residency ................................................. 6
  - Data sovereignty ............................................... 7
- Sovereign Cloud overview ............................................ 8
  - Data sovereignty and jurisdictional control .................... 9
  - Data access and integrity ..................................... 9
  - Data security and compliance .................................. 10
  - Data independence and mobility ............................... 10
  - Data innovation and analytics ................................. 11
- Sovereign Cloud value proposition ................................ 11
- Sovereign Cloud go-to-market strategy ............................ 12
  - Sovereign industry cloud ..................................... 12
  - Sovereign gov cloud .......................................... 12
  - Commercial cloud compared to Sovereign Cloud .............. 13
- VMware Cloud Provider partners .................................. 13
- VMware solutions and resources ................................... 14
  - VMware Cloud Provider Platform ............................. 14
  - Sovereign Cloud framework ................................... 14
  - Sovereign Cloud technical white paper ......................... 14
  - Compliance resources ......................................... 15
- Recommendations ...................................................... 16
Introduction

The VMware Sovereign Cloud framework is a set of guiding principles and best practices for delivering cloud services that can meet the security, compliance and data sovereignty requirements of a specific jurisdiction in which that cloud operates, as mandated by the relevant government or commercial body. This framework enables VMware Cloud Provider™ partners to successfully build and operate Sovereign Clouds that protect critical data for private sector and/or public sector organizations.

The primary goal of part 1 of this white paper is to help cloud provider executives, product managers, marketing and sales leaders, and cloud architects develop and position a Sovereign Cloud offering strategy. This paper addresses two questions: What is a Sovereign Cloud and why is it needed? Please note that no two Sovereign Clouds are the same. Every country (or region) has different requirements and interpretations around the scope of data privacy laws and a Sovereign Cloud. This paper presents a VMware perspective based on our interactions with cloud providers from around the world. It contains key concepts for partners to consider when designing and building a Sovereign Cloud strategy.

Part 2 of this white paper, a more technical piece targeted at cloud architects, focuses on how to design a Sovereign Cloud. Contact your VMware account team or aggregator to get your copy.

The information provided in this white paper is for informational purposes only and is not intended to constitute legal advice. VMware encourages its customers and partners to obtain appropriate advice from their own advisors on the implementation of all relevant data privacy laws, industry regulations, compliance requirements, and any other applicable requirements relevant to their business.

Emergence of data privacy regulations

Over the past two decades, several marquee events took place that put a spotlight on data privacy risks and the growing need to protect national, corporate and personal data.

First, there was an increase in public awareness related to how government authorities collect and use data about individuals across the globe. For example, in 2013, the U.S. National Security Agency (NSA) PRISM program was exposed, illustrating how the U.S. government was collecting vast swaths of data belonging to users of major internet services such as Gmail, Facebook, Outlook, and others. Similar global surveillance programs from other countries have also been identified, such as the Tempora program used by the United Kingdom’s Government Communications Headquarters (GCHQ).

Second, during this same period, the number of cybersecurity threats targeting private and public sector organizations grew exponentially. This culminated with the largest data breach in history in 2013–2014 when 3 billion user records were stolen from Yahoo. Two different attackers, which the company believed were state-sponsored actors, compromised the names, emails, dates of birth and telephone numbers of Yahoo users. In the U.S., a data breach costs a company on average $8.19 million ($242 per breached record).

In response to these surveillance programs, increased reliance on online platforms and technologies, and increased risk of cyberattacks, a growing number of countries have passed data privacy laws and regulations in the past decade. For example, the European Union’s General Data Protection Regulation (GDPR) sought to bolster online privacy rights following the increased utilization of online platforms and technologies, and to harmonize requirements across EU member states. GDPR applies to companies located in the EU as well as to those companies outside the EU that offer goods or services to EU residents.

Since 2018, many other privacy laws have emerged that draw some parallels to the GDPR. Brazil’s Lei Geral de Proteção de Dados (LGPD) restricts the collection, processing and transfer of personal data. In the United States, regulations are being passed at the state level, such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (VCDA). Similarly, privacy laws continue to emerge in Asia with draft legislation proposed in China (Personal Information Protection Law) and India (Personal Data Protection Bill). According to the United Nations Conference on Trade and Development (UNCTAD), 128 countries have legislation to secure data and protect privacy.

2. UNCTAD. “Data Protection and Privacy Legislation Worldwide.”
Data privacy is not getting easier

Organizations are struggling to understand and keep up with these global, regional and national data privacy regulations, especially when business operations span borders. In the coming years, industry experts expect data privacy to become even more complex.

First, data privacy laws continue to expand and change across the globe. Many countries are updating existing privacy laws to align to the standards set forth in GDPR. According to industry analysts, the majority of the world’s population will have its personal information covered under modern privacy regulations similar to GDPR.

New legislation has recently emerged that expands the scope of data privacy and raises new issues. For example, the CCPA expands the definition of personal information to include biometric data, browsing history, and geolocation. In addition, in 2018, the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act went into effect, which governs cross-border data access. This legislation was drafted in response to the Microsoft case that was pending before the U.S. Supreme Court at the time. This case related to emails stored in Ireland but controlled by a U.S.-based service provider. The provider argued that the reach of the U.S. court order stopped at the U.S. border. The CLOUD Act resolved this issue by stating that any service provider that is subject to U.S. jurisdiction, upon appropriate legal process, may be compelled to disclose data that is in that provider’s possession, custody or control, regardless of where the data is located. This type of legislation is not unique to the U.S. Similar legislation has been enacted globally, such as China’s Cybersecurity Law, the UK’s Crime (Overseas Production Orders) Act 2019, or Article 49 of the EU GDPR legislation.

There are also open questions about how regulators will interpret and enforce existing data privacy laws, such as the GDPR. In the summer of 2020, the Court of Justice of the European Union released its opinion on the Schrems II case, raising new questions about international enforcement and cross-border data transfers with non-EU states. The Schrems II decision invalidated the EU-U.S. Privacy Shield framework, rendering it an insufficient mechanism to ensure compliance with EU data protection laws.

The complexity of complying with privacy-related laws and protecting personal data is further exacerbated by the continued and growing risk of data breaches and evolving attack vectors. According to Statista, there were almost 1,500 cumulative data breaches in the United States alone in 2019, which exposed more than 164 million sensitive records. In 2020, there was a 400 percent increase in reported cyberattacks and an 800 percent increase in ransomware attacks due to the COVID-19 pandemic.

Lastly, data privacy requirements are driving data gravity. In other words, data and applications are attracted to one another. As critical data sets grow exponentially through new technology and business models, or as data gets repatriated back to sovereign soil, it’s increasingly necessary for applications to move to where the data resides to ensure performance. As a result, we see a growing trend in the cloud industry toward rapid expansion of commercial public cloud regions and/or toward adoption of locally or regionally delivered clouds.

As organizations embark on their cloud journey, they often have questions about security, the rights of foreign governments to access data, and how to ensure compliance with privacy-related regulations such as the GDPR when storing and sharing customer data. The local laws that apply in the jurisdiction where the content is located are an important consideration. However, organizations also need to consider whether laws in other jurisdictions may apply. These organizations are often confused about the differences between data residency and data sovereignty, including whether and in what circumstances any foreign authority may have access to their data. These challenges have led to the creation of new roles within organizations, including the chief data officer or data guardian. It also demonstrates the importance of conducting a data protection impact assessment (DPIA) and mapping data flows before adopting a cloud.

---

Growing need for Sovereign Clouds

Two major considerations drive the need for Sovereign Cloud and the overall market opportunity for VMware Cloud Provider partners.

Ensure data privacy

The first and most obvious driver for Sovereign Clouds is the need to comply with national or regional privacy-related requirements related to cross-border data transfers. End customers want to leverage all the benefits that cloud provides in terms of agility, elasticity and economics. However, they also need to meet the growing and evolving data privacy, legal and security requirements referenced earlier. Organizations need to maintain compliance with regional or national regulations that govern everything from where data resides geographically to cross-border data flow. Moreover, organizations need to protect data in the cloud against evolving attack vectors. In today’s complex computing environment, both private and public sector organizations continue to have legitimate concerns about the security of their data and third-party access to data.

![FIGURE 1: Protect and control critical data.](image)

Fuel innovation and economic growth

While data privacy is driving near-term demand, another major and growing consideration is the need to protect and fuel economic growth with Sovereign Clouds.

In the past five years, the geopolitical landscape has shifted significantly, and trust is becoming a rare commodity. We have witnessed growing trade disputes, friction between traditional allies, Brexit, growing suspicion of Big Tech monopolies, and the emergence of nationalism and populism across the globe. In 2020, the COVID-19 pandemic exposed the vulnerability and reliance that many nations/companies have on critical third-party supply-chain infrastructure and data services. In this context, there is growing concern about sensitive national, corporate and personal data being subject to the control of foreign authorities and companies.

Beyond the need to protect critical infrastructure, policy leaders increasingly recognize the criticality of data to enable economic growth and innovation. In the U.K., private and public sector leaders are evaluating ways to improve collaboration, decision-making and innovation by pooling national data. For example, the U.K. Automatic Number Plate Recognition (ANPR) system collects data from 11,000 cameras recording 50 million records per day. Combined with data from the U.K. Driver and Vehicle Licensing Agency (DVLA), this data not only enables law enforcement to identify the location of a stolen vehicle more quickly, but it also enables collaboration with universities for autonomous vehicle development, or local authorities in deciding where to build roads.

Increasingly, policy leaders see a need to build a national capability for digital infrastructure and resilience. As the data economy becomes a vital national interest, sovereign states need a digital capability that prevents them from becoming dependent on foreign powers and operators for processing their own data. According to the Atlantic Council, political leaders in both France and Germany have recently spoken about the need for “European champions” as an alternative to U.S. cloud providers. In September, French President Emmanuel Macron said, “the battle we’re fighting is one of sovereignty...If we don’t build our own champions in all areas—digital, artificial intelligence—our choices will be dictated by others.” Similarly, German Chancellor Angela Merkel expressed concerns about “digital dependencies” on the U.S.

6. Police.uk. “Automatic Number Plate Recognition (ANPR).”
To learn more about the growing need for national digital resilience, there is an excellent blog “Data must be treated as a national asset” from Simon Hansford, CEO of UKCloud and a thought leader in this space.

Perhaps the best example of this concept is the GAIA-X initiative in the European Union. The goal of GAIA-X is to develop a framework for a federated cloud and data infrastructure environment specifically for Europe that meets the highest standards of data sovereignty while also promoting innovation within the E.U. This framework includes the creation of federated GAIA-X hubs and data spaces that reflect the needs of user ecosystems at a European Level. The underlying premise of GAIA-X is to create an open, transparent digital ecosystem, where data and services can be made available and shared in a trusted environment. VMware is an active participant in the GAIA-X framework.

While the need for data sovereignty and Sovereign Clouds is not new, the concept has taken on new meaning and importance recently. Fundamentally, Sovereign Cloud is about the emerging data economy. It’s about protecting and unlocking the value of national, corporate and personal data. As acclaimed British mathematician and data scientist Clive Humby said, “data is the new oil.” Just as policy leaders have invested resources for many years in developing national highway infrastructure, airports or port facilities to foster economic growth, they must now invest in building a data economy.

Data residency and data sovereignty

Every customer (and partner) must define their own approach to data sovereignty and establish boundaries for data based on their legal interpretation of privacy laws and risk. To understand the trade-offs and risks, we must first define the difference between data residency and data sovereignty. These are related concepts that drive different cloud outcomes.

Data residency

Data residency refers to the physical and geographic location where customer data is stored and processed. This may be dictated due to policy, regulatory, tax or even performance reasons.

In general, this is what hyperscale public clouds provide when they build out regions in a specific country. At the end of 2019, the five largest hyperscale public cloud vendors had deployed 151 regions across 30 countries, representing 15 percent of the 206 states recognized by the U.N. Of course, the list of countries continues to grow rapidly as the hyperscale vendors start to target tier 2 and tier 3 markets.

In this scenario, customers have control over the boundaries of their data, what region(s) they use, and what services they enable. With a broad and deep service portfolio, hyperscale public clouds enable customers with all the self-service tools they need to deploy, manage and secure infrastructure in accordance with relevant government or industry regulations and compliance standards.

Although most public cloud services are segmented by region, there are some services that span regions and might easily and accidentally leak information across a sovereign border. For example, a company can accidentally violate GDPR because an unwary admin enabled cross-region replication for an object store full of personal data.

Assuming admins are diligent about their use of services, the potential risk with public clouds and data residency is twofold. First, while customer data may be resident, account information and metadata may not be. Second, resident data may be subject to compelled access by a foreign authority.

Customer data and account information

Hyperscale vendors make an important distinction between customer data and account information. In general, customer data is fully controlled by the end-user organization and is governed by the terms of agreement between the cloud provider and the customer organization.

However, account information is managed differently and is typically governed by a separate privacy statement. In the fine print, it often states that personal information may be stored in or accessed from multiple countries, including the United States. Moreover, these privacy policies typically state that account and other personal information may be released to not only comply with the law, but also to enforce or apply the terms of the customer agreement and other agreements. This type of statement is very broad and provides the hyperscale vendor with authority to control if/when data is released.

The amount of account information collected may also be much broader than most customers realize. While much of this data is provided by the customer themselves (e.g., name, email, address, phone, payment, organization, usernames, aliases, roles, etc.), a lot of metadata may be automatically collected with little customer awareness (e.g., network, IP, computer, device, credentials, streams, downloads, usage, errors, diagnostics, settings, preferences, backup information, API calls, and other logs). Lastly, some account information may even come from third-party sources (e.g., marketing, sales, search results, subscriptions, purchases, support, etc.).

Every customer should be familiar with the specifics of these privacy statements and what data is being collected directly, automatically and through other sources.
Distinguishing customer data from account information has two important implications. First, while customer data may be resident locally, other types of data, such as metadata or escalation data, may not be. Second, technical support for a local region of a hyperscale cloud is likely being delivered by system administrators in other countries, which potentially introduces some degree of risk.

Compelled access
Compelled access occurs when law enforcement or a national security agency for a government demands access to data (customer data or metadata) via legal means. It may also occur when a court orders that data be turned over due to litigation. Compelled access becomes a greater risk with cloud providers that are subject to U.S. jurisdiction due to the U.S. CLOUD Act discussed earlier. Of course, this risk is not unique to U.S. cloud providers. Any foreign-owned provider that is subject to U.S. jurisdiction, or any foreign-owned provider that is subject to other jurisdictions with similar laws, may also be subject to compelled access by a foreign authority.

For some customers, public clouds and data residency may be considered sufficient to comply with national privacy laws. The sheer fact that the data is local means it is subject to the data privacy laws of that country and therefore meets the minimum threshold required under those laws, even though metadata may not be resident and multiple jurisdictions may have authority over the same data. While this approach may provide customers with some comfort regarding compliance with cross-border data transfer requirements, customers should carefully consider the longer-term ramifications of storing confidential or restricted data in a foreign-owned public cloud, even if that cloud is available in a local region.

Data sovereignty
Data sovereignty refers to data being subject to the privacy laws and governance structures within the nation where that data is collected. Data sovereignty and residency are often conflated. Ensuring data sits within a geographical location for whatever reason (e.g., taking advantage of a tax regime) is a matter of data residency, while the idea that data is subject to the exclusive legal protections of a nation is a matter of data sovereignty.

This difference is critical because data subjects (e.g., any person whose personal data is being collected and processed) may have different privacy protections according to where the data centers hosting the data reside physically, and a government’s rights to access data within its borders differ from nation to nation.

Sovereign Clouds foster data sovereignty and jurisdictional control by addressing two critical requirements:

• Data is subject to the jurisdictional control and authority of the nation where that data were collected, and other jurisdictions are unable to assert authority over the data. This mitigates the risk and complexity of data being subject to multiple and overlapping legal standards.

• All data (e.g., customer data, metadata, escalation data, account information, etc.) are resident within that jurisdiction.

The first requirement is especially important when we think about enabling a national capability for digital resilience to protect critical government, corporate and personal data. To ensure the legal protections of a given nation, we must structure the cloud and its data flows (collection, transit, storage) so that other jurisdictions are not able to assert authority over that critical data.

In its simplest form, a Sovereign Cloud keeps all data collected within the national borders where that data was collected. This is typically seen in the public sector with government clouds or defense/intelligence clouds that hold classified and critical national data. In a few cases, hyperscale vendors do offer separate, air gapped gov clouds or defense clouds for select countries, such as the United States, that ensure all critical data remains within sovereign borders and those clouds are operated by staff/citizens with security clearances.

Ensuring that data remains within sovereign borders is not a unique concern of the public sector. In some countries, data privacy laws require private sector companies to keep a copy of the data within the country’s borders, usually to guarantee the government can audit its own citizens without having to contend with another government’s privacy laws. India’s Personal Data Protection Bill is an example of this. However, there are also countries where the law is so strict as to prevent data from crossing the border at all. For instance, Russia’s On Personal Data (OPD) Law requires all personal data be limited to data centers within the Russian Federation.

Increasingly, Sovereign Clouds must also recognize the growing need for cross-border data flows and the rapid emergence of hybrid and multi-cloud strategies. For example, a Norwegian banking institution may want to leverage a Sovereign Cloud in Norway for its primary business operations and critical data, but still access hyperscale public cloud resources in Asia for a mobile banking app, or hyperscale resources in Sweden for advanced analytics. In this example, we need to extend the concept of data sovereignty across borders.

To enable data sovereignty across borders, new concepts are emerging, such as virtual data spaces that comprise relationships between trusted partners that are governed by standards for secure and sovereign data exchange. This concept recognizes the need to share...
critical data to unlock innovation. The International Data Spaces Association (IDSA) is a coalition of more than 120 companies that are developing a global standard and certification process for international data spaces and interfaces that will enable the data economy of the future. Such a standard will enable data exchanges between trusted partners, across borders, and between clouds while still maintaining sovereignty.

One method for enabling a data space is to create a compliancy chain across cloud endpoints and to encrypt any data that resides in a foreign-owned cloud, while ensuring that the Key Management Server (KMS) remains under the control of the Sovereign Cloud provider or the customer themselves. In part 2 of this white paper, we will discuss how to extend data sovereignty in a multisite architecture that spans borders.

Regardless of the variety in these or other examples we could postulate, the core principle of maintaining jurisdictional control and authority over all data remains the same. Sovereign Clouds must enable a customer to define the boundaries of their own data (either within their own sovereign borders or across borders) yet maintain complete control and sovereignty of all data.

Sovereign Cloud overview
Sovereign Clouds help protect and unlock the value of critical data (e.g., national data, corporate data, and personal data) for both private and public sector organizations. This helps improve control of data, demonstrates compliance with privacy laws, and delivers a national capability for digital innovation.

Sovereign Clouds are about more than data sovereignty, though. While the location of data and jurisdictional control of data is important, Sovereign Clouds must provide customers with the confidence they need to deploy critical apps and data. Customers want assurances that all their sensitive data is properly managed, secured and controlled by a trusted cloud provider.

A Sovereign Cloud must have five characteristics to provide the assurances customers need:

- Data sovereignty and jurisdiction control
- Data access and integrity
- Data security and compliance
- Data independence and mobility
- Data innovation and analytics

As indicated in Figure 2 and the following section, each of these characteristics provide incremental value to the customer and enable the cloud provider to offer a more differentiated Sovereign Cloud value proposition.

While each cloud provider must determine the strategy and service portfolio that makes sense for their respective market, VMware believes a Sovereign Cloud should minimally meet the first three criteria around data sovereignty, data integrity, and data security. The remaining two criteria are optional capabilities that help drive more value for customers and therefore differentiation for partners.
Data sovereignty and jurisdictional control

At its core, a Sovereign Cloud is about data sovereignty and jurisdictional control. As previously discussed, a Sovereign Cloud must minimally ensure that data is subject to the jurisdictional control and authority of the nation where that data was collected, that other jurisdictions are unable to assert authority over the data, and that all data (e.g., customer data, metadata, etc.) is resident within the jurisdiction.

Data access and integrity

Beyond data sovereignty, a Sovereign Cloud must enable customers to access and consume their data with confidence to drive business outcomes.

To achieve this, a Sovereign Cloud should be deployed in at least two data center locations entirely under the jurisdictional control of the nation where the data is collected. These data centers should minimally align with a Tier III or higher data center classification from the Uptime Institute (99.982 percent availability or higher). In some cases, the Sovereign Cloud must be air gapped from other tenants into separate regions.

Minimally, the Sovereign Cloud must provide secure and private network connectivity with the ability to fully isolate the environment from the public internet. Typically, Sovereign Clouds will provide access to restricted networks. For example, in the U.K., a sovereign healthcare cloud might provide restricted access to the U.K. Health and Social Care Network (HSCN), while a sovereign government cloud might provide access to the U.K. Public Services Network (PSN).

Comprehensive data management and protection services is another minimum requirement for a Sovereign Cloud. It should offer customers a flexible portfolio of storage services, including options for immutable storage to ensure data can never be tampered with, modified, or removed. Immutable storage is especially important with the growing risk of ransomware attacks. In addition, a Sovereign Cloud should provide backup services with multiple copies of the data on different types of media, with at least one backup copy offsite. The Sovereign Cloud provider should also provide low latency connectivity across data centers for synchronous or asynchronous data replication.

More advanced services, such as database management, data loss prevention, and data lifecycle management, may also be provided. For example, end users have rights around their personal data, including the right to be forgotten. Data must therefore be classified and managed throughout the life of the data. When a user requests to be forgotten, procedures need to be in place to scrub the data. These advanced services enable cloud providers to drive higher levels of differentiation.

These services are well understood, and most cloud providers already offer these services. They are included only to highlight that Sovereign Cloud is a broader concept than data sovereignty. It includes the ability to ensure data access, availability, accuracy, consistency and validity.

FIGURE 3: Sovereign Cloud services cycle.
Data security and compliance

A Sovereign Cloud must provide the necessary security controls to protect data. These controls are typically designed around specific security frameworks and compliance standards. Figure 4 shows several examples from least to most stringent.

The minimum standard for a Sovereign Cloud is the Information Security Framework: ISO/IEC 27000-series, or any similar standard. Specifically, ISO 27001 dictates 114 controls across 14 categories and provides a framework to implement an information security management system (ISMS). This allows providers to secure data through a risk management process that combines people, processes and systems. While ISO is a well-known global standard, there are also regional standards, such as SecNumCloud (France) and BSI C5 (Germany). For providers targeting public sector or defense, a standard such as NIST SP 800-53 High would be recommended. Data sovereignty, integrity, and security controls should be audited annually by a third party, using SSAE 16/ISAE 3402 or the equivalent.

Beyond establishing an ISMS and certifying the underlying cloud infrastructure, cloud providers should also develop a portfolio of value-add security services. The Cloud Security Alliance provides guidance on developing a security-as-a-service portfolio. In the context of Sovereign Cloud, the two most important security services that providers should offer are network security and data encryption.

Network security is critical because of the need to potentially isolate the Sovereign Cloud from the outside world. Beyond providing secure and private network connectivity and protecting the perimeter of the data center, the cloud provider must also enable micro-segmentation for east-west traffic within and across data centers to enable a Zero Trust security posture that only allows explicit traffic to transit the network.

The Sovereign Cloud must also provide disk and virtual machine (VM) level encryption with a sovereign KMS that remains under the control of the customer or the trusted Sovereign Cloud provider. This is particularly relevant for cross-border data transfers because, typically, the Sovereign Cloud will not exist in isolation. There may be cases where the customer needs to extend their business into clouds in other regions. In this example, data sovereignty is maintained if we encrypt the data that crosses borders but retain control of a sovereign KMS.

Data independence and mobility

A key tenant of Sovereign Cloud is the ability to avoid any dependency on foreign vendors (including hyperscalers), while at the same time being able to use them when needed without the risk of customer data or metadata being exposed. A Sovereign Cloud should empower the customer to deploy and move applications and data when and where needed as business conditions change, including full reversibility to prevent cloud vendor lock-in.

One way to do this is by enabling workload migration between sites, ideally without having to change the application. In fact, it should be just as easy to move workloads out of the cloud as it is to move them into the cloud in the first place. This, of course, requires a common architecture across sites to enable seamless portability and interoperability. Another approach to portability is by enabling modern, container-based applications that can be deployed on any cloud infrastructure. There is a growing trend toward “cloud around” strategies that enable modern apps to be deployed anywhere using Kubernetes as an abstraction layer.
Data innovation and analytics
A Sovereign Cloud should also help customers unlock the value of their data to drive business innovation. Cloud providers should invest in building out a portfolio of advanced data services, such as data lakes, data warehouses, AI, or machine learning (ML) services, to deliver more value and differentiation around their Sovereign Cloud. Customers need these platform services to uncover insights and achieve competitive advantage.

For cloud providers that lack these capabilities, another approach to innovation is by enabling data to be shared or extended to other clouds without sacrificing data sovereignty. For example, leverage the advanced analytics and data services that hyperscale public cloud platforms provide to derive insights around anonymized data, while maintaining and protecting the source data with a Sovereign Cloud. As previously noted, this can be accomplished by creating a data space that spans borders, clouds, and companies. Accordingly, the Sovereign Cloud should be flexible enough to accommodate multisite design across hybrid or multi-cloud when needed.

Sovereign Cloud value proposition
For end customers, Sovereign Clouds deliver several benefits.

<table>
<thead>
<tr>
<th>SOVEREIGN CLOUD BENEFITS</th>
</tr>
</thead>
</table>
| Improve control | • Keep data under sovereign control and jurisdiction  
| | • Prevent compelled and authorized access to data by foreign authorities |
| Improve security | • Secure infrastructure, apps and data against rapidly changing attack vectors  
| | • Implement industry best practice security controls more quickly and effectively |
| Improve compliance | • Achieve compliance significantly faster and more efficiently  
| | • Demonstrate compliance on an ongoing basis, rather than every few months |
| Unlock data | • Share and extend data with trusted nation-states, companies, or clouds  
| | • Leverage advanced services to enable data analytics and insights |
| Future proof | • Protect against changing data privacy regulations, security threats and geopolitics  
| | • Avoid cloud vendor lock-in with workload, app and data portability |
| Fuel innovation | • Pool national, corporate and personal data to unlock economic growth  
| | • Build a national capability for digital resilience for the data economy |

For government policy leaders, the last point is critical. Sovereign Clouds help mitigate the risk of concentration and dependency on U.S. hyperscale public clouds. Increasingly, industry and government leaders are shifting from a cloud-first to a cloud-smart strategy that embraces multi-cloud and mitigates cloud vendor dependencies.

This does not mean that customers should stop using hyperscale public clouds. On the contrary, these clouds provide tremendous value in the breadth and depth of services offered. Rather, customers should classify their data and apps, and develop a multi-cloud strategy that leverages the right cloud for the right workload.
**Sovereign Cloud go-to-market strategy**

With a better understanding of Sovereign Cloud, we must also recognize there are different go-to-market strategies. For example, some may think of Sovereign Clouds as synonymous with gov clouds that only target the public sector, but the concept is broader and applies equally to the private sector.

**Sovereign industry cloud**

One go-to-market strategy that is becoming increasingly common is to offer a sovereign industry cloud that targets a specific private-sector vertical industry with sensitive and proprietary data that is often regulated. This typically includes verticals that are vital to the national interest and economy, such as financial services and banking, utilities and telecommunications, or healthcare and pharmaceuticals. These types of industries are often subject to specific industry compliance standards and regulations that often vary by nation/region.

For example, for U.S.-based financial services organizations, the Office of the Comptroller of the Currency’s Heightened Standards for Large Financial Institutions, the Federal Reserve’s Enhanced Prudential Standards, and the Federal Financial Institutions Examinations Council (FFIEC) Information Technology Handbook serve as the foundation for risk management. In Europe, regulations for financial services organizations are codified through MiFID II, Basel IV, LIBOR cessation, Solvency II, and various other European Banking Authority (EBA) guidelines.

A sovereign industry cloud may be delivered as a private and/or public cloud that meets the five characteristics previously described. Often, data protection and security services are embedded or bundled into the service (e.g., backups, disaster recovery, encryption, micro-segmentation). A sovereign industry cloud may also offer compliance as a service with proactive and continuous monitoring, reporting and remediation against compliance drift. While hyperscale public clouds offer a full portfolio of security and compliance services, the burden is on the customer to ensure proper use of these self-service tools. Sovereign industry clouds, on the other hand, typically deliver an integrated solution with broader accountability to the end customer.

Sovereign industry clouds go by many names. They may also be referred to as a community cloud, regulated cloud, or compliant cloud. Regardless of the positioning, the concept is the same: offering a trusted cloud that ensures security and compliance with specific data privacy laws and commercial regulations.

The same concepts previously discussed regarding data residency and sovereignty apply to industry clouds. For example, Microsoft Azure provides industry clouds for healthcare, retail, financial services and more. IBM Cloud for VMware Regulated Workloads targets the financial services industry. While these hyperscale clouds provide a broad set of services, customers should assess whether all their data, including metadata, is controlled by one or more jurisdictions. Hence, it’s important to distinguish between industry clouds and sovereign industry clouds.

**Sovereign gov cloud**

Another go-to-market strategy for Sovereign Cloud is to target the public sector with a gov cloud.

A sovereign gov cloud provides everything a sovereign industry cloud provides and more. For example, it will typically be deployed into separate, air-gapped availability zones and cloud regions on sovereign soil. It usually requires that all data and services remain within sovereign borders, prohibiting cross-border data flows. Additionally, many governments require that a sovereign gov cloud be operated by certified staff with security clearances, typically citizens. In some cases, even tenant users will be screened to gain access. Another common characteristic is to provide access to restricted government networks, such as the U.S. NIPRNet or the U.K. PSN. Lastly, the compliance standards for public sector will vary by nation. In the U.S. alone, a sovereign gov cloud may need to demonstrate compliance with FedRAMP, FISMA, FIPS, CJIS, CCPA, and more.

Depending on the nation, a sovereign gov cloud will target different market segments. Minimally, this could include federal/central agencies, state/provincial agencies, and local government. In some countries, public sector may also include education and healthcare. While public sector may be the primary target market, cloud providers can also target private sector organizations that are doing business with the public sector.
Commercial cloud compared to Sovereign Cloud

The following chart shows how a Sovereign Cloud can be executed with different go-to-market strategies, and how each use case compares to commercial public clouds.

<table>
<thead>
<tr>
<th>GTM AND POSITIONING</th>
<th>PRIMARY MARKET</th>
<th>SECONDARY MARKET</th>
<th>JURISDICTIONAL CONTROL</th>
<th>LOCAL DATA CENTERS</th>
<th>LOCAL CLOUD LEGAL ENTITY</th>
<th>METADATA IN COUNTRY</th>
<th>NATIONAL OPS/STAFF</th>
<th>NATIONAL CAPABILITY</th>
<th>SECURITY SERVICES</th>
<th>DATA TYPE CLASSIFICATIONS VARY BY COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUBLIC CLOUD</td>
<td>Private Sector</td>
<td>Public Sector</td>
<td>Data Residency</td>
<td>Varies</td>
<td>Varies/Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Optional Security</td>
<td>Public Data, Consumer Data, Unclassified data, Protected Data</td>
</tr>
<tr>
<td>INDUSTRY CLOUD</td>
<td>Private Sector</td>
<td>Public Sector</td>
<td>Data Residency or Data Sovereignty</td>
<td>Yes</td>
<td>Yes</td>
<td>No/Yes</td>
<td>No</td>
<td>No</td>
<td>Embedded Security</td>
<td>Corporate Data (IP), Confidential Data, Sensitive Data, Regulated Data</td>
</tr>
<tr>
<td>GOV CLOUD</td>
<td>Public Sector</td>
<td>Private Sector</td>
<td>Data Sovereignty</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Optional Security</td>
<td>National Data, Official Data, Restricted Data</td>
</tr>
<tr>
<td>DEFENSE CLOUD</td>
<td>Public Sector</td>
<td>n/a</td>
<td>Data Sovereignty</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Embedded Security</td>
<td>Classified Data, Secret Data, Top Secret Data</td>
</tr>
<tr>
<td>PRIVATE CLOUD</td>
<td>Private or Public Sector</td>
<td>n/a</td>
<td>Data Sovereignty</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Customized</td>
<td>Varies</td>
</tr>
</tbody>
</table>

VMware Cloud Provider partners

VMware Cloud Provider partners are well positioned to deliver Sovereign Clouds. First, they often have a better understanding of local, national, or regional security and compliance requirements as well as government policy objectives and initiatives. Second, they can design, build and operate a tailored cloud for a specific jurisdiction, ensuring all data and services remain under sovereign control. Third, if properly structured as a sovereign organization, the cloud provider can develop a national capability for digital resilience and mitigate dependency on U.S. operators. Lastly, VMware Cloud Provider partners can serve as a trusted multi-cloud advisor to end customers. Many of these cloud providers support both VMware-based clouds and non-VMware clouds, including hyperscale public clouds. This makes them uniquely qualified to guide the customer on their journey to hybrid and multi-cloud.

Today, VMware has more than 4,000 cloud provider partners that have a local/regional presence in more than 120 countries. Combined, these partners manage more than 10 million VMs for more than 160,000 customers. This provides customers with the broadest choice in deployment venues for sovereign workloads.
VMware solutions and resources

VMware Cloud Provider Platform

The VMware Cloud Provider Platform enables cloud providers to design, build and operate public, private or hybrid cloud (infrastructure as a service [IaaS]/platform as a service [PaaS]) services in provider data centers that align to the five Sovereign Cloud characteristics previously described. This enables cloud providers to build a cloud tailored to the unique needs of each market. Moreover, cloud providers can then extend this platform into other cloud endpoints, such as customer data centers, colocation data centers, edge locations, or even hyperscale data centers using the same technology.

<table>
<thead>
<tr>
<th>Solutions</th>
<th>VMware Cloud Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted Private Cloud</td>
<td>Public Cloud Migration</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Containers as a Service</td>
</tr>
<tr>
<td></td>
<td>Security/Compliance</td>
</tr>
<tr>
<td></td>
<td>Custom Services</td>
</tr>
</tbody>
</table>

FIGURE 5: VMware Cloud Provider Platform.

The VMware Cloud Provider Platform is a proven technology stack for delivering a modern, software-defined cloud. Leveraging a common architecture across endpoints, VMware-based clouds can often provide the fastest, easiest and lowest cost solution for cloud migration. With bidirectional workload portability and infrastructure interoperability, VMware-based clouds should be an integral part of any customer’s hybrid or multi-cloud strategy.

Sovereign Cloud framework

To help cloud providers design Sovereign Clouds, VMware is developing a Sovereign Cloud framework.

This is an emerging framework of guiding principles and best practices for delivering cloud services that adhere to the data sovereignty requirements of the specific jurisdiction in which that cloud operates as mandated by the relevant government or commercial body. The framework is intended to be flexible enough to accommodate different design considerations depending on the scope of the Sovereign Cloud. This white paper is part of the Sovereign Cloud framework. Contact your VMware account team to learn more about this framework.

Sovereign Cloud technical white paper

The goal of part 1 of this white paper is to explain what a Sovereign Cloud is and why it’s important to cloud providers, customers, and policy leaders. Part 2 of this white paper, a more technical piece, is intended to provide high-level guidance on how to design a Sovereign Cloud given that requirements and scope will vary across cloud providers.

Building on the concepts introduced in part 1, part 2 will provide a conceptual framework for designing a Sovereign Cloud. As indicated in Figure 6, each layer of the Sovereign Cloud stack drives requirements that are addressed by the characteristics (or services) of the layers below in a flexible and modular way. This concept allows providers to design Sovereign Clouds that allow for cross-border data flow or that strictly limit data boundaries to sovereign soil.
Within this framework, we must understand the business requirements that drive the architecture. This includes assessment of any compliance requirements and risk as well as defining the scope of our data boundaries.

We can then design the data sovereignty layer by enabling policies across apps and data, and by leveraging micro-segmentation and encryption to create data boundaries and control data flow between locations. This is where we create a data space or sovereign domain that might span endpoints.

And, finally, we can deploy infrastructure into a specific locale and create policies for a residency domain. In some cases, the residency domain may be the same as the sovereign domain, but in other cases, it could be different to allow for cross-region data transfer. This modular approach provides design flexibility for partners.

FIGURE 6: Conceptual framework for designing a Sovereign Cloud.

Compliance resources
VMware has several resources to help cloud providers design and implement security controls for different compliance standards; for example, the VMware Validated Design™ Compliance Kit for PCI or NIST 800-53. These kits include a Product Applicability Guide that maps product features to specific controls, including VMware Cloud Director™.

Moreover, the VMware Compliance Controls Database, which leverages the Unified Compliance Framework (UCF), can be used to map security controls from different compliance standards to a single, common control. This makes it possible to build one security control that helps achieve multiple compliance standards, improving efficiency and time to value.
Recommendations

For customers, VMware recommends the following:

• Identify if there is a national data strategy for your country and develop a plan that aligns to this.
• Engage a trusted partner to conduct an application, data discovery, and data protection impact assessment before adopting a cloud. Develop an app, data, and cloud migration strategy.
• Shift from cloud first to cloud smart by deploying the right workload into the right cloud (i.e., multi-cloud).
• Leverage clouds that mitigate all risks for critical data (security, compliance, and data sovereignty risks).
• Contact a local/regional VMware Cloud Verified partner to help guide you. Find a VMware Cloud Provider.

For cloud providers, VMware recommends the following:

• Research your market to understand national/regional privacy laws and data strategies/initiatives.
• Engage with customers to identify requirements and use cases, and to educate them on Sovereign Clouds.
• Engage with government policy leaders about building a national capability for the digital economy.
• Leverage assets in the Sovereign Cloud framework to design, build, promote and sell a Sovereign Cloud value proposition.
• Contact your VMware account team or aggregator to define and execute a Sovereign Cloud strategy.

You can also visit cloudsolutions.vmware.com or engage with us on social media to learn more.