

Building Trust With Sovereign Cloud: **How Governments Can Safeguard Their Data**



Governments and the Cloud:

Meeting the Unique Challenges Governments Face When Using the Cloud

Cloud is the great enabler—and that is not an exaggeration. It gives businesses a chance to thrive, to move ahead, and to be a step ahead. It opens pathways to a myriad of benefits, all with the end goal of improving the bottom line and making the organisation better.

Little wonder then that cloud use has been on the uptick in recent years, so much so, that USD \$289.7 billion in 2020. In addition, as much as 74% of global IT decision-makers say that 95% of all workloads will be in the cloud by 2025, while 60% say they will have the majority of their IT in it in the next two years. Even small business owners seem to be recognising the value proposition of the cloud, with around 78% of them adopting the cloud in the last three years.

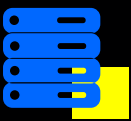
In other words, organisations of all shapes and sizes—and in practically all verticals and industries—are turning to the cloud.

But what, exactly, is the cloud?



The Cloud Deciphered

The cloud, or more accurately, cloud computing refers to the delivery of computing services over the Internet rather than through expensive hardware and software. These services include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), and each offers unique benefits to businesses.



Infrastructure-as-a-Service is the most basic level of cloud computing. It provides businesses with access to virtual machines, storage and networking resources so they can quickly and easily spin up new servers and storage resources as needed—all without having to invest in expensive hardware. This helps businesses be more agile and responsive to the different situations they may encounter.



Platform-as-a-Service provides businesses with a complete platform for building, deploying and managing applications. This helps the business develop and deploy important applications quickly and easily, without having to worry about managing the underlying infrastructure.

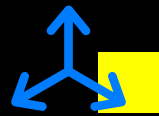


Software-as-a-Service gives businesses access to fully managed software applications, like Salesforce and Microsoft Office without having to worry about installing or maintaining the software themselves.

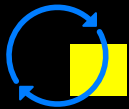
Among The Benefits of Leveraging The Cloud Are:



Cost savings. With cloud computing, businesses only pay for the resources they actually use, without having to invest in expensive hardware and software upfront.



Scalability. With cloud computing, businesses can easily scale their resources up or down as needed, depending on their workload.



Greater flexibility and agility. With cloud computing, businesses can quickly spin up new resources as needed, allowing them to be more responsive to changing conditions and arising situations. In addition, businesses can easily access their data and applications from anywhere in the world since they are stored on the Internet.



Improved security. Cloud providers typically invest heavily in security measures, such as firewalls, intrusion detection systems and data encryption, in order to protect their customers' data.

In short, it pays to be using the cloud. It can be very good for business.

Governments Can Benefit From the Cloud Too

While the cloud is generally associated with business use cases, governments can benefit from being in the cloud just as much. In fact, in this digital age, a government needs to at least have parts of its services in the cloud if it wants to serve its constituency better, faster and more efficiently.

No less than the World Bank has vouched for cloud use in the public sector, noting [in a feature article back in 2022](#) how “cloud services play a critical role in accelerating digital transformation and delivering essential public services.”

The World Bank cites as an example the dire COVID-19 situation in Rwanda, which was further exacerbated by a lack of healthcare professionals. Helping augment this shortage of healthcare workers, according to the World Bank, was Artificial Intelligence (AI)-assisted medical triage “using a cutting-edge application that required a connection to the cloud.”

This modern, hi-tech, cloud-enabled application checked Rwandan patients using a symptom checker and then monitored them afterwards, in turn freeing up Rwanda’s strained medical staff to support others. This same AI-driven solution also helped with near-real-time language translation that allowed patients to speak their language.

To that end, the case for governments around the world to leverage the cloud is actually quite simple—and logical. Doing so is the next stage of digital transformation, and it can enable governments to provide important services as demonstrated in Rwanda during the height of the pandemic. On top of that, being in the cloud, as already discussed, grants governments access to a multitude of sophisticated SaaS applications that can, in turn, be used to address different public sector challenges. Moreover, being in the cloud means governments can leverage cloud-based backup systems that can help ensure redundancy should their physical system crash. This, in turn, ensures service continuity.

Closer to home, governments in Southeast Asia are also adopting cloud-first strategies to varying degrees and for a range of purposes. The Philippines, for instance, has been transitioning to the cloud as early as 2017 with the [launch of GovCloud under the Philippine government's Cloud-First policy](#). The initiative proved just in time, as it allowed the Philippine government to keep its core services available online even during the pandemic when nationwide lockdowns were imposed during the COVID-19 health crisis. Today, many of the Philippine government's services are available online via the cloud, facilitating easier, more convenient transactions between the government and citizens.

Nearly the same scenario is playing out in Malaysia, [whose MyGovCloud Initiative is a crucial component of the Fifth Initiative](#) under Malaysia's Digital Economy Blueprint. Its aim is to accelerate the digital transformation of Malaysia's public sector and, at the same time, stimulate the country's growing digital economy. Such cloud-centric initiatives are nothing new in governments here in Southeast Asia and worldwide, and they will continue to be implemented moving forward given the enabling benefits of being in the cloud.

Despite, these obvious benefits, there are also challenges when it comes to using the cloud. And, for governments, those challenges mainly centre around data—the need to protect and secure it, in particular, and the need to follow regulatory and compliance requirements in storing it.

Data Make Cloud Adoption Trickier for Governments

Among the biggest concerns with using the cloud is that an organisation gives up a degree of control to someone else—or something else, in this case. An organisation that uses cloud services essentially entrusts its data to a third-party service provider—say, Google Cloud, for instance, or Amazon Web Services—that manages and stores said data on its servers.

This setup, and the degree of control over data surrendered in the process, raises concerns about data control and ownership. This is particularly true for governments, who generally are in possession of their citizens' most sensitive personal information, like driver's licence details, social security numbers and other similar data. People entrust these pieces of information to their government, with a level of expectation that these will be secured, protected and kept private. There is also an expectation that this data is sovereign, or subject to the privacy laws and governance structure within the country where it is located in the first place.

To give a better idea of what the Sovereign Cloud is all about, consider the case study that is TikTok versus the US government.

Case Study

TikTok VS the US Congress

The US Government has been actively trying to ban TikTok, the social media app, the former has been actively trying to ban the social media app on US soil on speculations that it will, upon prodding from the Chinese government, share user data with the Mainland, thereby compromising the integrity and privacy of millions of accounts. In response, and to avoid a complete ban on a large market, TikTok developed Project Texas, whose sole purpose is to keep the data of all US-based subscribers in the US and out of China's reach.

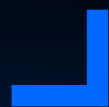
Project Texas, run by US-based TikTok subsidiary TikTok US Data Security Inc. (USDS), encapsulates the concepts of the Sovereign Cloud because it is specifically designed to keep in US soil the data collected by TikTok from US-based users. It will also be governed by a board of directors vetted by the US Committee on Foreign Investment in the United States (CFIUS), further ensuring that said data will not be subject to foreign compromise.



The bottom line is this:

American data stored on American soil by an American company overseen by American personnel.... Only vetted personnel vetted in the new company, called Tiktok US Data Security, can control access to this data...

Shou Zi
CEO, Tiktok



That is the ideal scenario for governments wishing to leverage the cloud: to be able to keep their own data outside the reach of other entities outside national and territorial boundaries.

Not for nothing, **countries around the world are strengthening their data protection laws.** For instance, countries in the European Union are subscribed to the strict and encompassing General Data Protection Regulation (GDPR). Canada, on the other hand, has the Digital Privacy Act, while China and Australia are governed by the Personal Information Protection Law and the Privacy Act, respectively.

Unfortunately, while public clouds generally keep data private and secure, they might not necessarily cover the data sovereignty part of the equation—and that might be a deal-breaker for governments looking to extend their reach to the cloud. But the issue is not so much about cloud service providers not being subject to strict regulations and compliance requirements because they are; the question is whether or not those regulations and requirements are aligned with those of the host country whose government is using the cloud.



Enter, the Sovereign Cloud

Organisations today want complete authority and jurisdiction over their data, even if it is in the cloud—a demand buoyed in part by a growing belief that confidential data remains vulnerable in a public cloud. This demonstrates a critical need for a secure, fully compliant cloud where data access is confined to specific geographic boundaries only.

That is the gap [AVM Cloud](#) is trying to fill with Sovereign Cloud solutions powered by VMware, which is among the first companies to explore the concepts of Sovereign Cloud. AVM Cloud, a subsidiary of TIME dotCom Bhd, launched in February 2023 [its Sovereign Cloud solutions](#), which are anchored on the multi-cloud technology of VMware and promise organisations using it the full benefits of multi-cloud use—all while complying with data residency and sovereignty regulations. In other words, these solutions built on the Sovereign Cloud are built specifically to deliver security and data access that meets the strict requirements of regulated industries and local jurisdiction laws on data privacy, access and control.



What is Sovereign Cloud?



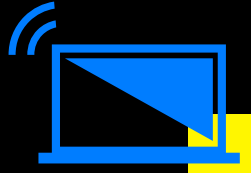
Operated by
a sovereign entity



Only national state
has jurisdictional
control of data



All data is resident
and/or controlled in
the jurisdiction



Foreign authorities
cannot assert authority
over data



Operation & management
carried out in a sovereign
territory

With the principles of Sovereign Cloud, governments are ensured of data sovereignty and jurisdictional control, which means:

- There is an autonomous legal operating entity in the jurisdiction and no affiliate relationships that can subject data to outside interference.
- Foreign authorities or legal entities will not be able to assert any authority over that data.
- Data is subject to the exclusive jurisdictional control and authority of the government's jurisdiction.
- All data is resident and controlled in that jurisdiction.

“

The massive opportunity of the data economy now demands sovereignty over data. With rising concerns over privacy protection, AVM's certified Sovereign Cloud will be a game changer for both the public and private sectors in their efforts to control and protect highly critical data while maintaining compliance with local regulations across regions and multiple cloud environments.

KIT AU

Executive VP of Enterprise Business, TIME dotCom Bhd

There is a huge demand for Sovereign Cloud solutions in Malaysia and around the world because organisations today are storing and stewarding data from customers beyond one market in order to drive innovation and growth.

Partners like AVM help ensure all data, workloads and processes are kept within the country and in full adherence to local data residency and sovereignty regulations, which in turn empowers enterprises to focus their efforts and resources on business outcomes with the full confidence that they are working within a secure and compliant cloud infrastructure.

SARENE LEE

VMware Country Manager, Malaysia

”

Put simply, the concept of the Sovereign Cloud matters now more than ever because of the following concerns:



Evolving data-related laws and regulations



Growing geopolitical friction



Concern for digital sovereignty



Fuel sovereign economic growth

Geopolitical friction, in particular, has become a big concern given the increasing conflicts between countries, political uncertainties and countries growing suspicious of other countries, as demonstrated in the case between the US government versus China (by way of TikTok). Concern for digital sovereignty is also growing exponentially in the era of big data and social media, with the latter, in particular, demonstrating the ease with which data can cross international borders.

AVM Cloud's different solutions on the VMware-developed Sovereign Cloud address these key issues by providing these key value propositions:

Improved security

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

Greater control over data

- Ensure visibility and auditing of all cloud administration and activities.
- Prevent unauthorised or authorised access to data by foreign entities.

Future-proofing the organisation

- Keep up with changing regulations, security threats and geopolitics.
- Avoid vendor lock-in.

Improved compliance


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

Unlock the value of data


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

Economic innovation

- Develop a national and sovereign digital capability.
- Pool national data to unlock economic innovation and growth.

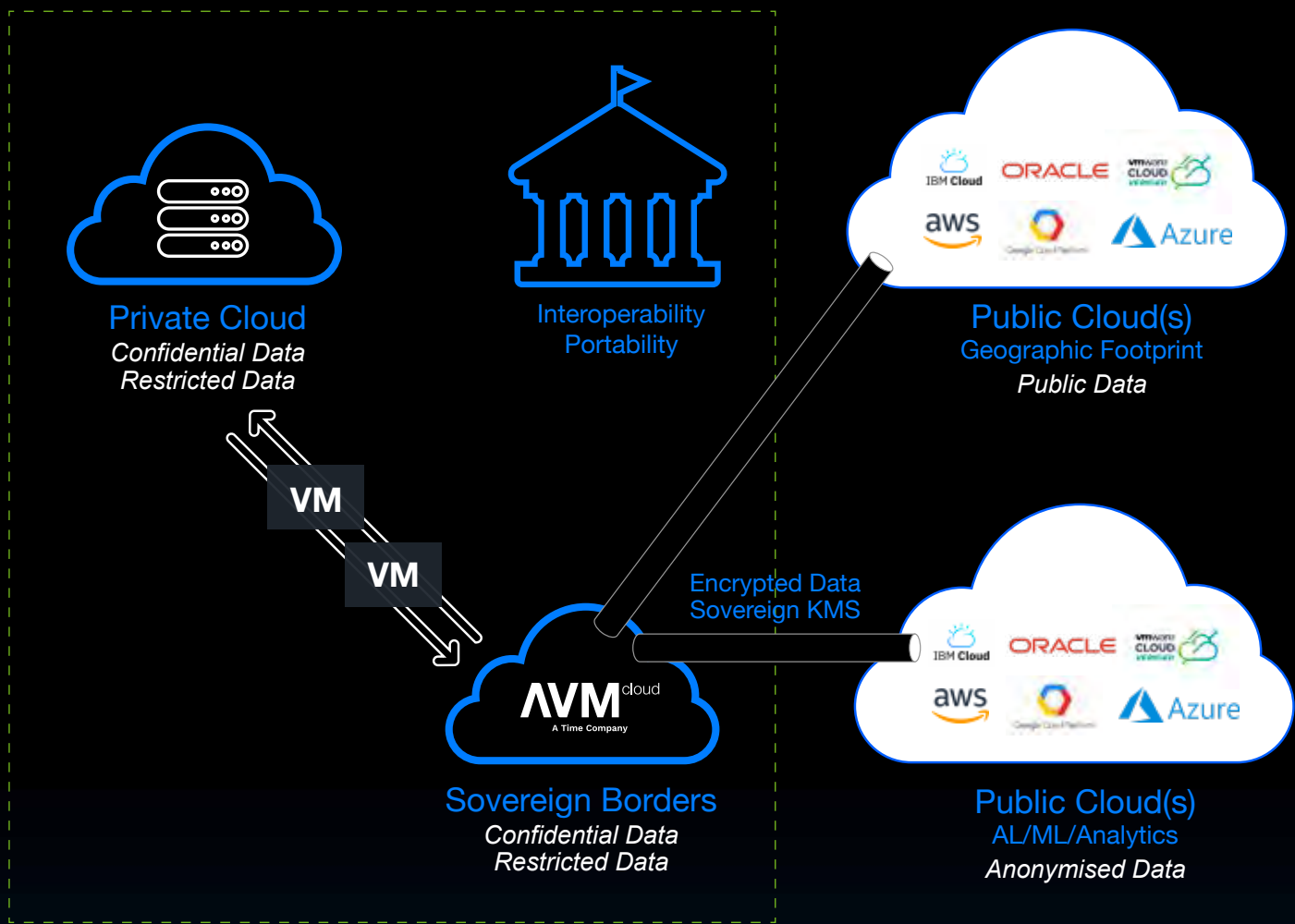


A key element to AVM Cloud's solutions in the Sovereign Cloud is that they support multi-cloud setups, augmenting hyperscale public clouds to allow organisations to better leverage the multi-cloud. It also enables cross-border data sharing when necessary, but maintains data sovereignty all the while.



Here is a graphical representation of how Sovereign Cloud principles augment the public cloud in a multi-cloud environment:

Sovereign Borders



Sovereign Cloud: The Cloud Paradigm for Governments

For governments specifically, AVM Cloud offers various solutions in the Sovereign Cloud that are very similar to a commercial cloud (i.e., AWS, Microsoft Azure, etc.) but provide these additional features and characteristics:

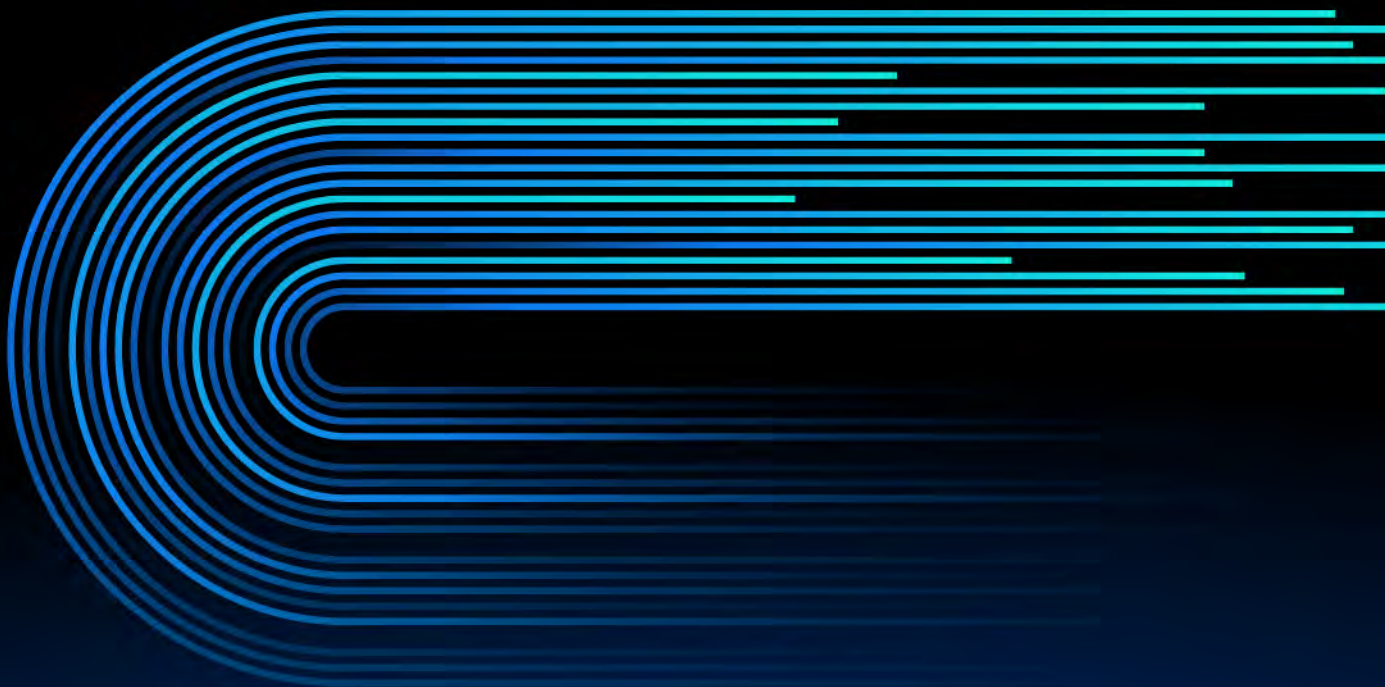
- It operates on air-gapped cloud regions deployed on sovereign soil.
- All data and services are kept on sovereign soil.
- It is operated by certified staff—typically citizens with security clearance.
- It operates on restricted network connectivity (government networks).
- It provides public sector GTM, contract vehicles and business processes.

Organisations need to recognise their unique needs in order to maintain the utmost levels of data privacy, protection, and handling. One of the most important factors for successful transition to cloud computing is having the right cloud partner who can get you on the right track.

AVM Cloud pioneered Cloud Computing Services in Malaysia in 2010 and has since established itself to be on par with global cloud service providers. With our years of experience, AVM Cloud's compliance and legal teams have developed comprehensive privacy controls to restrict the level of personal information visible and accessible.

Put simply, AVM Cloud's Sovereign Cloud solution allows governments and the public sector in general, to derive maximum value from being in the cloud and, at the same time, ensure data sovereignty for sensitive personal data.

It is the best of both worlds, and it is exactly what governments need in this digital age.





AVMcloud

A Time Company

AVM Cloud logo is the trademark of AVM Cloud Sdn Bhd.