Publication date:
06 Sep 2023
Author(s):
Dennis Hahn, Principal Analyst, Data Center Storage;
Roy Illsley, Chief Analyst, IT Operations;

Sovereign Cloud – Part Two: How Technology Vendors are Approaching its Delivery

OMDIA
Brought to you by Informa Tech

Table of Contents :

Summary

Catalyst

In 2023 the term “sovereign cloud” is being used by many technology vendors to describe how their solutions deliver data privacy and data residency. This report is the second on the topic of sovereign cloud and profiles some of the different approaches technology vendors have taken to delivering it. Part One defined the key attributes and levels of a sovereign cloud, and in Part Two the vendor offerings will be evaluated. It will cover cloud service providers (CSPs) as well as software vendors. The analysis will focus on describing how their offerings deliver sovereign cloud capabilities or support the sovereign cloud concept.

Omdia view

The approach to delivering a sovereign cloud—or digital sovereignty as it is also known—differs significantly between the vendors included in this report. Some of the offerings are based on the core capabilities of the vendor’s existing public cloud architecture with very little modification or any new offerings beyond some packaging and go-to-market modifications. Other vendors have developed entirely new offerings and packages and market these as specific sovereign cloud solutions. Omdia’s research made it clear that one approach to sovereign cloud is to understand the geographical sovereignty requirements by understanding the local regulations and concerns. Building any sovereign cloud from this base would deliver a solution that meets the Level 4 requirements of extraterritorial access. However, another approach is to look at the CSP’s technology and apply it to meet the sovereign cloud needs of the vendor and its customers. Building a sovereign cloud in this way would enable a cloud provider to deliver a solution faster, though this solution might not provide extraterritorial access protection. These two approaches demonstrate that in addition to being able to meet the expectations of nations, there is a commercial aspect to delivering a sovereign cloud, and most cloud providers have solutions that fit into either camp.

Though motivations and approaches to delivering sovereign cloud differ, there is a common acceptance that it is not something the large vendors can do alone. The use of local trusted partners is key to any delivery strategy, but this use must be designed so that it meets requirements, particularly in delivering a cloud that is free from extraterritorial access. Much of the focus is on how any sovereign cloud will operate in Europe, but that is not the only potential market, and vendors need to build solutions that are repeatable globally based on the differing requirements of different geographies.

Key messages

- The technology vendors’ approach falls into two main camps.
- It is necessary to understand the different levels of digital sovereignty.
- Customers adopting sovereign cloud plan to do so in 2023 and 2024.
- Delivering a sovereign cloud is all about trust, transparency, and openness.

Recommendations

- **Understanding the local requirements is the starting point for any sovereign cloud.** Different regions and countries have different regulations on what being sovereign means. Therefore, it is important that any solution begins with an understanding of these requirements and then maps them to the vendor offerings.
- **Sovereign cloud must be commercially viable.** The delivery of any sovereign cloud must pass two basic tests. First, does it meet the customers' expectations? Second, can this level of sovereignty be delivered in an efficient manner? The wider ecosystem of partners and the supply chain must also be considered. There is no point in vendors developing a gold standard solution that customers cannot afford, because the alternative is to move those workloads and data back on-premises.
- **Local trusted partners are the key to delivering any sovereign cloud.** The level of sovereignty required by the EU means that the large hyperscalers, or any non-EU vendor, will need to think carefully about how they deliver their sovereign clouds. The key protection that local trusted partners can deliver for these companies is protection of data from extraterritorial access.

Understanding the market

Technology vendors' approaches fall into two main camps

Omdia has conducted a number of interviews and briefings with the leading technology vendors on the topic of sovereign cloud. They all claim to have a solution that delivers on the core functionality of sovereign cloud, but their approaches fall into two main camps.

Sovereign by design

This group of vendors all use the argument that the core design philosophy of their solution delivers the capabilities needed to deliver a sovereign cloud. The technical details of how they deliver this differ, but the core premise is that the data is secure with access controls and policies that ensure it remains within the country and compliant with local regulations. The other common trait of this secure-by-design approach is its approach to protect against the US Cloud Act: either the vendor has a transparency ethos, or the vendor states that it has no access to customers' data. Under the "transparency" approach, the vendor records and publishes requests for access to data and the number of times data was provided. The vendors have different views on what legal actions they are prepared to take to stop the data being handed over, but these actions appear to be limited to challenging the request in the US courts. Vendors whose employees have no access to customer data do not explicitly state how they would respond to a request for access by law enforcement.

Built to be sovereign

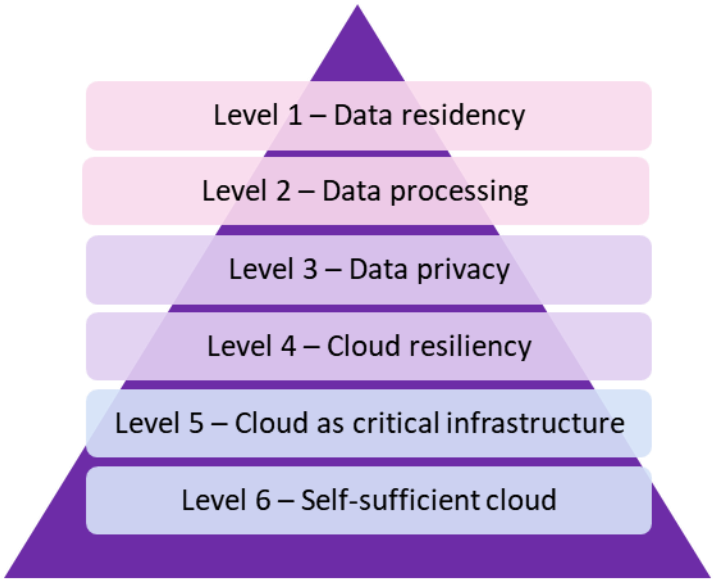
This group of vendors have all taken their existing capabilities and built a specific sovereign solution. The main difference with this approach from the sovereign-by-design school is that these solutions are built to be sovereign by having specific features that "air gap" the US-owned vendors from the US Cloud Act. The argument for this approach is that this is how the sovereign-by-design vendors deliver US federal services, but they are not prepared to deliver, or feel the demand does not warrant, the same for other countries. It

is clear that adopting this approach (built to be sovereign) is more costly: it requires separate facilities that are isolated, both physically and logically, from the public cloud network.

The Omdia sovereign cloud model

The first report covered this in more detail, but it is included here for reference and as a reminder. **Figure 1** shows the six-level model; the vendors in this report are only targeting their sovereign cloud at the top four levels. Omdia believes these top four levels will account for 100% of commercial customers, with only a few countries being interested in or capable of operating at Level 5 and beyond, mostly for top-secret government activities, which are out of the scope of this report.

Figure 1: Omdia's model for sovereign cloud



Source Omdia

The six-level model follows a logical progression from the core principle of any digital sovereignty, which is that the data remains resident in the country. The next level expects that data to be processed in the country, but neither of these two levels applies any controls specifically on who does the processing and how; it is purely about processing being performed in the country. At Level 3 the controls are about who can access the data, what restrictions are placed on the processing, and how extraterritorial access can be denied. Level 4 moves the requirements beyond just a single sovereign cloud to cover how cloud resiliency can be protected in the country or region and how the country or region can continue to make use of cloud computing in the event of geopolitical sanctions.

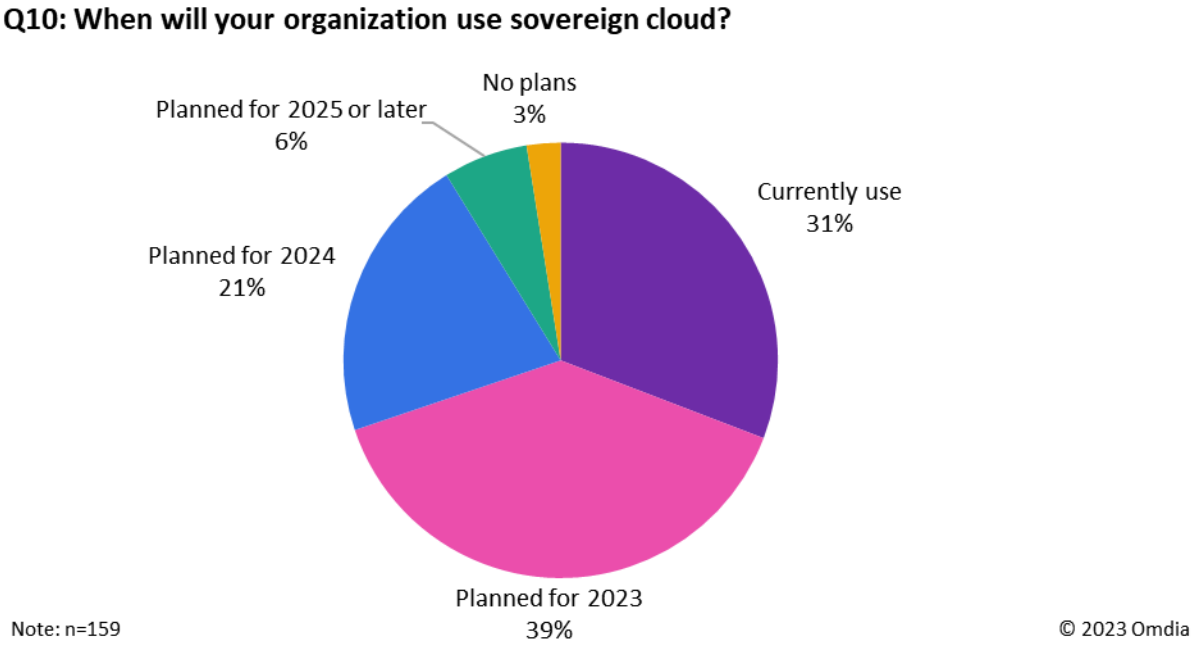
Sovereign cloud market analysis

Omdia's cloud services survey

Omdia conducts an annual cloud services survey, and in 2023 we asked specifically about sovereign cloud. **Figure 2** clearly shows that it is a topic of great interest for 2023: 60% of organizations globally report plans

to use sovereign cloud by the end of 2024. In fact, 31% are already using sovereign cloud, which Omdia believes is mostly on-premises private-cloud-like deployments. But with 57% of enterprises reporting that they are using industry clouds, there is room for growth.

Figure 2: Sovereign cloud intentions of enterprise customers



Source Omdia

Interestingly, Europe, Middle East & Africa (EMEA) is not currently the largest user of sovereign cloud. It is the lowest user, with only 25% of respondents, while in Asia & Oceania, 36% of respondents report they are currently using sovereign cloud, and in North America the proportion is 31%. However, if all intentions are converted to actual usage, then by the end of 2023 Asia & Oceania will remain the largest market with 74% using sovereign cloud, followed by North America with 70%, and EMEA with 65%. However, these results must be viewed in light of the fact that the EMEA respondents were from a range of countries across the region and included a majority from non-EU countries, which may explain EMEA's low adoption figures. As expected, the regulated industries (e.g., financial services) are currently the largest users of sovereign cloud, with 88% expecting to be using a sovereign cloud by the end of 2023. In contrast, only 14% of retail respondents report that they are currently using it. It is no surprise that the drivers for using sovereign cloud are a requirement for data processing within the country boundaries and on for data privacy, meaning citizens' data must be stored in the country. It is interesting that data privacy was the top reason in Asia & Oceania, and data processing was the top reason in North America. EMEA had both as joint top reasons. This indicates that in Asia data localization is more important, whereas in North America it is more about who has access to process the data, while EMEA considers both aspects equally.

How the different technology vendors address the requirements of a sovereign cloud

It is all about trust, transparency, and openness

The different approaches espoused by technology vendors are evaluated in this section; six different vendors' solutions are profiled. The aim is to show how these different approaches work and to map them against the Omdia sovereign cloud model (see **Figure 1)**. However, Omdia does not expect any vendor to discuss its approach to Level 5 or Level 6, because this would involve divulging agreements with governments on topics such as the transfer of IP and ownership of assets, which is out of scope for this report aimed at enterprise customers. Another aspect that is still a work in progress for European companies is the recent EU-US Data Privacy Framework and the OECD's Declaration on Government Access to Personal Data held by Private Sector Entities. The creation of a forum for cooperation in digital trade through the Trade and Technology Council is a step in the right direction, but despite this real progress the story is not yet over.

NetApp BlueXP takes a data-centric approach to delivering digital sovereignty

NetApp would not be the first company many people would think of when considering adoption of sovereign cloud. However, if we stop and consider what being sovereign is all about, NetApp does become a natural company to add to the list, because NetApp's approach is to focus on the data, which is at the heart of any sovereign cloud considerations. NetApp BlueXP delivers the core capabilities and functionality needed to ensure data privacy, not just for a single cloud but in a hybrid multicloud environment. The NetApp BlueXP philosophy is based on ensuring data can be managed so that it complies with any specific regulatory demands. NetApp BlueXP unifies NetApp's storage and data services under a single control plane. BlueXP allows customers to discover, deploy, and operate storage in a range of different environments including AWS, Azure, and Google Cloud Platform (GCP) public clouds and on-premises. The key operating principle is that all these environments can be managed via a single control plane. The key technology supporting NetApp's approach is its ONTAP operating system.

NetApp ONTAP

The ONTAP operating system is used in many of the storage products and services that BlueXP can manage and provide data services for. At a high level, ONTAP provides comprehensive resiliency, availability, and serviceability features. These include built-in data protection, encryption, replication and cyber-resiliency. One of the design principles of ONTAP is that it can reduce operational costs through simplification of the management tasks. The other storage products that BlueXP works with include

- **Cloud Volumes ONTAP:** software-defined ONTAP service using public cloud infrastructure-as-a-service (IaaS) storage
- **Amazon FSx for NetApp ONTAP:** fully managed storage service offered by AWS, based on ONTAP
- **Azure NetApp Files:** fully managed file storage offered by Azure, based on ONTAP
- **Cloud Volumes Service:** ONTAP delivered as a fully managed service for GCP

ONTAP uses a number of key capabilities to ensure it can deliver the management of data irrespective of whether it is on-premises or in the public cloud. These include the capabilities listed below.

Redundant array of independent disks (RAID)

RAID is a standard method of protecting data from any single disk drive failure by distributing the data over multiple disk drives. ONTAP supports both RAID-DP, where two drives are used, and RAID-TEC, where three drives are used. RAID delivers data resiliency in multiple copies so that data is not lost because of a hardware failure of a disk drive.

Write Anywhere File Layout (WAFL)

The issue with RAID is it introduces performance degradation because of the need to write the data two or three times. WAFL delivers a solution to reduce the impact of adopting RAID by using full stripe writes. A full stripe write allows the controller to calculate new parity using new data being written to the drives. There is almost no write penalty, because the controller does not need to read old data from the drives to calculate the new parity. As the size of the array grows larger, the write penalty is reduced by the ratio of p/n, where p is the number of parity drives and n is the total number of drives in the array.

Storage virtual machines and thin provisioning

ONTAP uses the concept of storage abstraction where the storage administrator can create logical data pools across different physical drives. Thin provisioning is another industry standard capability that enables the storage to be allocated dynamically as needed. The advantage of this approach is that storage does not need to be preallocated to an application, which leads to low storage utilization.

Clustering

A cluster consists of one or more nodes grouped together as high-availability pairs. The advantage of creating a cluster is that it enables the nodes to pool their resources and distribute work across the cluster. From a management perspective, the cluster is a single entity to manage and as such can be created in a way to create a resilient sovereign data store. The maximum number of nodes within a cluster depends on the platform model and licensed protocols. Each node in the cluster is able to view and manage the same volumes as any other node in the cluster. One of the key advantages in a sovereign use case is that the nodes in a cluster communicate over a dedicated and physically isolated Ethernet network that provides a level of separation needed to ensure data is not leaked.

Quality of service

Having the data securely isolated is one key aspect of meeting the needs of data sovereignty, but it must also be possible to manage the performance and balance the resources. ONTAP delivers an adaptive quality of service where it automatically maintains the ratio of input/output operations per second (IOPs) to terabytes per second as the demand changes.

BlueXP deployment modes

NetApp has three deployment modes for BlueXP that deliver different degrees of data privacy and, by implication, sovereignty.

Standard mode

In standard mode, BlueXP is deployed as a SaaS offering and encrypts the data that is transmitted over the public internet. Because it is a SaaS offering the service is provided and managed by NetApp; updates are delivered automatically. Standard is not considered to be a solution that will meet most sovereign cloud requirements.

Restricted mode

The restricted mode is analogous to Levels 1 and 2 in the Omdia model for sovereign cloud and provides granular control of the flow of information. The key capability in restricted mode is that communications are controlled by an intermediate stage, the BlueXP Connector. The Connector is located within the sovereign cloud region and will have only outbound unidirectional connectivity to the BlueXP SaaS backend, and it initiates all communications with the BlueXP SaaS layer. The services that are supported in restricted mode include Cloud Volumes ONTAP, Amazon FSx for ONTAP, Azure NetApp Files, BlueXP backup and recovery (Cloud Backup), BlueXP classification (Cloud Data Sense), BlueXP digital wallet, on-premises ONTAP clusters, and BlueXP replication (SnapMirror). However, currently this offering is not universally available in all regions with access to all of NetApp's services and cloud resources.

Private mode

In private mode, the BlueXP SaaS layer is not used because there is no outbound connectivity required. This mode can be deployed in a restricted cloud region (such as AWS C2S/SC2S or Azure IL6) or in an on-premises environment and allows local authentication only. The BlueXP user interface (UI) and API are served locally and do not allow the use of BlueXP's SaaS-based UI. Any BlueXP updates are carried out manually because all packages, components, and dependencies are within the Connector and remain stored on the local virtual machine. The number of services available in private mode is reduced and is also different between on-premises and cloud. For cloud deployment BlueXP backup and recovery (Cloud Backup), Cloud Volumes ONTAP, BlueXP digital wallet, and on-premises ONTAP clusters are supported. For on-premises deployment BlueXP backup and recovery (Cloud Backup), BlueXP classification (Cloud Data Sense), BlueXP digital wallet, on-premises ONTAP clusters, and BlueXP replication (SnapMirror) are supported.

Analyst opinion

Though NetApp may not be the first name that comes to mind when sovereign cloud is considered, it has a long history of data management and storage. With BlueXP and the different deployment modes it has developed a solution that provides a single control plane and that can be used to meet different regulatory requirements. However, the NetApp solution is not a comprehensive sovereign cloud solution: it covers the data and who can see it, where it can be stored, and how/whether it can be moved. It does not provide an answer to the question of whether the infrastructure aspect of the private cloud complies with sovereign cloud requirements; it is the customer's responsibility to check and ensure compliance.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com