AWS Ticks All the Boxes with Digital Sovereignty Pledge — Now it Needs to Make it Work in the Real World

December 08, 2022

By: Rahiel Nasir, Archana Venkatraman, Giovanni Cervellati, Rick Villars

IDC’s Quick Take

True digital sovereignty is difficult to implement, but organizations around the world are demanding solutions that address evolving sovereign assertions and expectations. AWS wants to get ahead of the game here, with new commitments to expand its solutions for cloud sovereignty, and all without compromising on features, availability, or agility. The challenge for the company now is to turn all its pledges into a practical reality.

AWS' Digital Sovereignty Pledge

With its recently announced Digital Sovereignty Pledge, AWS is promising to expand on its current range of data protection features to give customers what's claimed to be the "most advanced" sovereignty controls available in the cloud.

The company plans to invest in what it describes as an ambitious road map of capabilities for data residency, granular access restriction, encryption, and resilience in an effort to expand on the existing "sovereign-by-design" capabilities of the AWS Cloud. It adds that all this will be done without compromising on the capabilities, performance, innovation, and scale that cloud can offer.

AWS highlights four key focus areas in its road map.

Firstly, as part of giving customers greater control over data location, the company says it will provide more fine-grained data residency controls and transparency, along with expanding data residency guardrails for operational data, such as identity and billing information. It has already added data residency controls into AWS Control Tower in a bid to give customers greater control over the physical location of where their data is stored and processed.

Secondly, AWS has enhanced the confidential computing features of Nitro, a collection of building blocks that underpin its Elastic Compute Cloud (EC2) computing services. Nitro is said to use specialized hardware and software to protect data from outside access during processing so that nobody, including AWS personnel, can access customer workloads unless authorized. The firm adds that it remains transparent about how its services process and transfer data, and that it will continue to challenge requests for customer data from law enforcement and government agencies.

Thirdly, AWS has committed to invest in features that will enable customers to encrypt all data everywhere, whether in transit, at rest, or in memory, using keys that are managed inside or outside the AWS Cloud. This will be supported by the recently announced availability of the AWS Key Management Service or XKS.

Finally, the company pledges to boost its options for resilience, enabling users to continue operations through disruptions or disconnections. The AWS Cloud currently spans 96 Availability Zones (AZs) within
30 Regions globally. According to the company, the multiple AZs within its regions are fully isolated infrastructure partitions, and to better isolate issues and achieve high availability, it says customers can partition applications across multiple zones in the same region.

**IDC's Point of View**

IDC research shows that the geopolitical and economic storms of disruption that are currently impacting organizations across the world have heightened global interest in digital sovereignty solutions.

What's more, we see interest in digital sovereignty now growing beyond the traditional regulated sectors where organizations are primarily driven by compliance needs. As cloud usage grows across all industries, and organizations keep more of their sensitive data in public clouds, many are seeking sovereign solutions to help alleviate concerns about data security, privacy, and control over data access.

With its pledges around data residency and giving customers greater control over the location of their data, AWS has a solid starting point. The company points out that there is no data lock for customers in its cloud, and this is worth shouting about — as it further invests in its data portability capabilities, the firm would do well to amplify this to help bolster customer trust. AWS believes transparency about how its services process and transfer data is key to earning that trust, but fears over vendor lock-in — which can be exacerbated by a lack of data portability and limiting the customer's need to multisource — can weaken any trust that has been built up.

According to IDC, control over access to data by a cloud service provider's administrators is the priority for organizations globally when it comes to working with sovereign solution partners (source: *Future Enterprise Resilience and Spending Survey, Wave 4, May 2022*). Once again, AWS strikes the right chord here with a promise to expand its controls over access to data by its own personnel such as administrators and support staff. But how issues of identity and access management will actually work in the real world with an organization that is headquartered in the U.S. (and therefore outside the jurisdiction of cloud users in other parts of the world) will need to be spelled out.

Digital sovereignty is ultimately about risk and resilience, as shown in the IDC Sovereignty Stack. Indeed, business continuity is one of the top two priorities for organizations looking to invest in partners for digital sovereignty. AWS' pledge here is to enhance the resilience of the multiple AZs that make up each of its cloud Regions, enabling customers to sustain operations through disruption or disconnection. The firm adds that to better isolate issues and achieve high availability, users can partition applications across multiple AZs in the same AWS Region. This is certainly a worthy and welcome pledge, but what's not clear is how much control AWS or its customers have over the technical and operational layers of the sovereignty stack, such as the networks that interlink all the datacenters in an AZ, and indeed the datacenters themselves.

With organizations already grappling with multiple clouds and hybrid IT estates, adding sovereignty to the cloud strategy adds yet further complexities. AWS acknowledges this and is also aware that sovereignty needs will vary across industries and countries, and as rules and regulations continue to evolve. Partnerships are vital here, not only between providers and customers, but also between providers and partners. AWS says it would never expect its customers to "go it alone" and will work with trusted partners in individual markets to support customers.
This is a good approach as sovereignty success is based on working in an ecosystem. However, the challenge for providers is to assure customers that not only do they offer guaranteed sovereign credentials, but that their partners also do so, and that also applies to the partner’s partner, and so on. Furthermore, it is an ongoing process and a shared responsibility, as all stakeholders will need to continually ensure they remain sovereign across their relevant operations. This requires investment in the management and monitoring skills and tools that can be used by all parties, and over the long term.

Stifling digital innovation is a possible side effect of implementing a sovereign cloud which, by its very nature, tends to be one with restricted cloud features. Here, AWS pledges to innovate on sovereignty features, controls, and assurances within its global cloud. The company acknowledges the complexity of meeting ever-evolving and expanding sovereignty requirements while maintaining its rich feature sets. It believes that customers should not have to choose between the "full power" of AWS and a feature-limited sovereign cloud solution that could hamper their ability to innovate, transform, and grow. How AWS will achieve this remains to be seen. But in the meantime, one of the firm’s biggest concerns around delivering sovereign cloud capabilities through regional partnerships is to ensure it can maintain its public cloud secret sauce.

And then, of course, there’s the question of price. A sovereign cloud is, by its very nature, a limited cloud because of all the data, infrastructure, operational, etc., restrictions that are applied to it. Many organizations would therefore find paying more for less hard to justify. As an example, many cloud users in Europe — a region that is likely to experience the greatest impact from AWS’ pledge — say they would not be willing to pay a premium of more than 20% of their cloud budgets for a sovereign cloud solution (source: IDC EMEA, Multicloud Survey 2022, September, August 2022).

AWS ultimately talks about expanding its "sovereignty by design" capabilities, but how it plans to do this on a practical level as part of its standard cloud offerings remains to be seen. Nevertheless, IDC believes the market should move to "sovereignty by default" and, as with security, the question over whether it is needed as an optional and chargeable extra should not arise.

However, if AWS ultimately succeeds in putting its ambitious plans into action, it could not only catch up with rivals but also help provide a template of how the full stack of digital sovereignty components can move from being a concept to a workable, real-world operating model.

Further reading: T-Systems, AWS Launch Data Protection as a Managed Service to Help Cloud Adopters Adhere to EU Data Regulations While Accelerating Cloud Journeys (IDC #EUR149070722, May 2022)