Exposure of Data in the Cloud Induces Greater Risk of Data Corruption and Data Theft

Antoine Viale, Michael Maicher and Rohan Thomas

ISG WHITE PAPER

INTRODUCTION

Public cloud has become an indispensable tool for enterprises to scale efficiently and store data. Because of globalization, however, enterprise data can be stored in datacenters situated in other geographic regions. This means data is not only governed by different regional laws, but it is also susceptible to cybersecurity attacks depending on the vulnerability of the datacenter.

In 2016, the European Union adopted the General Data Protection Regulation (GDPR), which later became enforceable in 2018. As it is a regulation and not a directive, the GDPR is malleable with each member state of the union having a different version of the directive. The GDPR was an important steppingstone that guaranteed data privacy to EU citizens; since its enforcement, regional governments across the EU have collected fines of over €1 Billion. It has also served as a framework to nations outside the EU to guarantee data privacy and security. The sovereign cloud builds on GDPR by enhancing the sovereignty of data originating from inside the region.

On July 16, 2020, the Court of Justice of the European Union (ECJ), in its Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (called "Schrems II case"), invalidated the EU-U.S. Privacy Shield with immediate effect. In March 2022, both regions agreed with the court's decision about new principles for "Privacy Shield 2" with the adoption of proportionate surveillance activities and an independent adjustment mechanism. However, many organizations based in Europe and the U.S. lacked a legal basis for their transfers of personal data.

Sovereign Cloud: What is it all About?

The idea behind the sovereign or trusted cloud was to give teeth to the GDPR and ensure that only residents have access to their data, barring intermediary service providers, including cloud service providers.

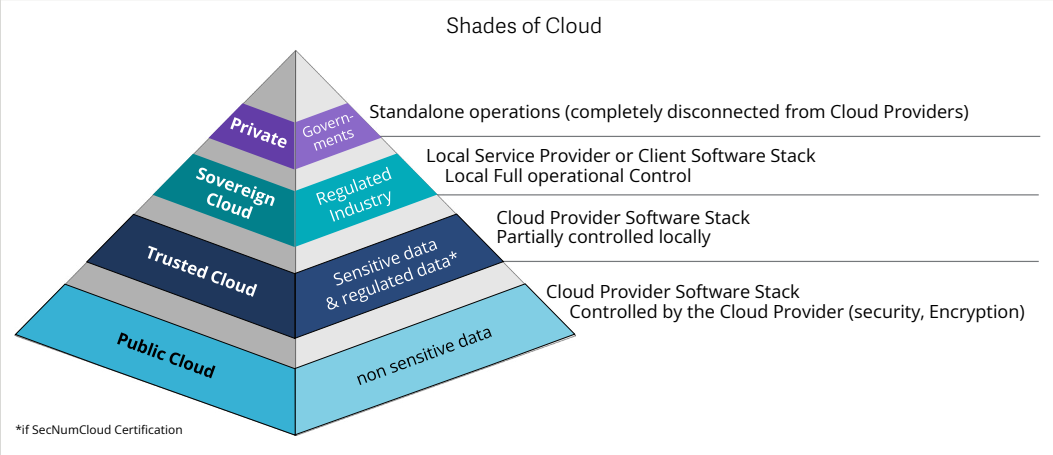
Sovereign or trusted clouds can be readily deployable, allowing enterprises to migrate critical data into the environment without concerns about business implications. It enables data residency and localization, ensuring that the data is governed, managed and stored based on EU compliance laws.

In addition to pushing for data residency and localization, the sovereign cloud is built with significantly lesser reliance on vendor software or hardware and thus reduces vendor lock-ins while increasing interoperability. In this way, it enhances transparency among stakeholders and restricts interference from vendors, service providers or other third-party entities.

Who needs the Sovereign or Trusted Cloud?

While the sovereign cloud is important for government agencies that hold confidential information, critical industries that are subject to higher levels of industry-specific regulations are increasingly adopting the platform. Global enterprises that have a presence in the EU are also embracing it to ensure compliance with data regulations in the region.

Figure 1: Gradiant of Sovereignty: From Public Cloud to Private



Source: ISG

The Gaia-X Project

The sovereign cloud is in its formative years, with EU member states implementing their own rules to meet regional requirements. Many initiatives have been introduced to bring its capabilities to fruition, one among being the Gaia-X project.

Initiated by Europe for 181 member states, the project was launched to design the next generation of sovereign cloud data infrastructure built completely on open-source software. According to ISG's 2021 Cloud Native Study, while 41% to 52% of respondents considered data storage and adherence to relevant policies important, only 2% of them expect Gaia-X membership from their cloud service providers.

Present State of European Public Cloud Market

The European public cloud market is consolidated, with Amazon Web Services (AWS), Microsoft Azure and Google Cloud continuing their dominance. These hyperscalers have control of 75% of the Infrastructure-as-a-Service (IaaS) market in Europe and collectively spent well over €12 Billion in 2021 to upgrade their regional hyperscale data centers. European cloud service providers had a smaller market share (just 3%) with Deutsche Telekom, Europe's leading native-cloud service provider.

Exposure of Data in the Cloud Induces Greater Risk of Data Corruption and Data Theft

The challenge thus lies in the inability of regional cloud service providers to scale up in an industry dominated by those of foreign origin and to serve industries that should adhere to data sovereignty requirements. This would otherwise translate into high costs for the end user of the sovereign cloud.

How should Enterprises, Public Institutions and Service Providers Acclimatize to the New Mandate?

There has been a considerable push by EU governments to adopt regional hybrid cloud providers such as Dassault Systèmes, Thales and OVHcloud as a way to promote data residency within the EU. To alleviate costs and enhance scalability, these cloud service providers partner with trusted hyperscalers to provide a best-of-breed approach for the sovereign cloud. Scaleway, a subsidiary of the French Iliad group, is the first European IaaS provider to offer a high-performance sovereign cloud ecosystem based on its own software stacks.

Another noteworthy example also includes the integration of Thales, OVHcloud, Indra and T-Systems with Google to deliver sovereign cloud to enterprises in France, Germany and Spain. Primarily built for France, Bleu is another example of this approach wherein Orange and Capgemini have partnered with Microsoft Azure.

While such partnerships and integrations can significantly help alleviate costs, sovereign cloud solutions still cost an average of 20% more than traditional public solutions. ISG thus recommends that end users start by confirming the capabilities of their existing cloud solutions meet their requirements. End users should thus review the available sovereign cloud solutions to ensure they match their business and growth requirements.

ABOUT THE AUTHOR

Exposure of Data in the Cloud Induces Greater Risk of Data Corruption and Data Theft

ANTOINE VIALE

Partner, Strategy and Sourcing Advisory

Antoine's background includes more than twenty-five years of progressively responsible positions in Business and High-Technology services companies. He is a talented and accomplished senior management professional, highly skilled in complex IT Strategy engagements and large transformational deals. He has established and directed highly successfully, multi-million dollar Information Technology programs for large fortune 500 companies (Alstom, AXA, AXA Technology Services, BNPP Corporate Investment Banking, Bridgestone, Carrefour, Crédit Agricole, Dassault-Aviation, EDF, Givaudan, HSBC, Alcatel-Lucent and Nokia, Renault-Nissan, Sanofi, TEVA Pharmaceuticals, Total…). He has negotiated more than $4 billion in proposals and contracts.

ABOUT THE AUTHOR

Exposure of Data in the Cloud Induces Greater Risk of Data Corruption and Data Theft

MICHAEL MAICHER

Service Line Director, DACH

Michael advises his clients on the development and implementation of business-oriented IT strategies, comprehensive IT sourcing strategies as well as ramp-up and operation of transformation programs. He supports medium-sized and large companies in organizing and carrying out tendering and negotiation processes for IT services (ADM and IT infrastructure). In addition, Michael advises CIOs and IT managers on the strategic realignment and redesign of IT organizations (role of IT, target operating model, structural organization, IT governance and IT processes and roles). In addition, he has concrete experience in change management as well as in coaching IT executives. Michael has developed 360-degree assessments for selected IT management functions and successfully applied them in customer projects, e.g., project and application portfolio, enterprise architecture management as well as sourcing and change readiness assessments.

ABOUT THE AUTHOR

Exposure of Data in the Cloud Induces Greater Risk of Data Corruption and Data Theft

ROHAN THOMAS

Senior Lead Analyst

Rohan Thomas has a Masters of Technology Degree in Computer Aided Design and Manufacturing (CAD/CAM) from the Vellore Institute of Technology, India. Rohan brings to the job close to a decades' worth of experience in communications technology, hardware & semiconductors, and communications testing. At ISG, Rohan is a knowledge expert on the adoption of the cloud and has done extensive research on the Private and Hybrid in France and the Benelux.

ABOUT ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, www.isg-one.com.

Let's connect NOW...