Google Cloud

January 2025

Take control of your digital future with Google Sovereign Cloud

Organizations worldwide remain hesitant to adopt foreign cloud services due to three primary concerns. First, concerns around data control, where evolving regulations and the potential for foreign government intervention raise questions about who has ultimate access to sensitive information. Second, concerns around economic dependency and the need to reduce risk driven by a lack of domestic cloud service providers. Third, the need to proactively plan for potential geopolitical disruptions that could cut off access to critical data and services.

These three concerns underpin the growing global demand for what is known as **digital sovereignty** and define Google's approach to addressing these concerns. According to Gartner, by 2025, 10% of global businesses will operate more than one discrete business unit bound to and by a specific sovereign data strategy.[1]

This whitepaper details how Google Sovereign Cloud — a comprehensive set of controls across Google's public cloud services, Google Distributed Cloud, and Google Workspace — enables every organization to meet their data, operational, and software sovereignty needs so they can accelerate their digital transformation with confidence. We showcase how we are empowering customers with more local solutions, flexible workload controls, and robust security, to serve the increasingly diverse digital sovereignty requirements.

[1] Source: Gartner Top Trends in Cybersecurity for 2024, January 2024 - ID G00802944

What is driving the need for digital sovereignty?

Organizations are increasingly embracing cloud technologies to support their digital transformation initiatives. However, concerns around data control, economic dependency, and geopolitical disruptions hinder cloud adoption, particularly in the public sector and regulated industries.

Data control concerns

Governments everywhere are creating stricter rules about where data can be stored and who can access it. In France, for example, the French National Cybersecurity Agency (ANSSI) SecNumCloud initiative requires that important government data, as well as data from critical industries, be stored and managed within Europe. Meanwhile, the United States, with its U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, allows law enforcement to reach across borders and compel American companies to hand over data, no matter where it's stored. The European Union has a similar approach with its e-Evidence Regulation, enabling cross-border access to electronic evidence for law enforcement purposes.

These evolving laws create a complex landscape for companies, forcing them to carefully consider where they store data and how they control access to comply with these regulations.

Economic dependency concerns

Uneven distribution of technology and the concentration of major cloud providers in the U.S. raise concerns about potential economic imbalances and dependence. This is driving the demand for solutions that rebalance operational capabilities across the world and partnerships that empower domestic players to oversee or operate technology in a way that ensures trust.

Geopolitical concerns

Geopolitical tensions are spilling over into the digital world, driving nations to assert greater control over their data and online infrastructure. This pursuit of digital sovereignty is fueled by the need to protect sensitive information from foreign surveillance and ensure uninterrupted access to critical digital services in disruptive geo-political scenarios. By managing their digital assets locally, countries aim to ensure survivability, safeguard national interests, boost local tech industries, and reduce their reliance on foreign entities.

Google Cloud's approach to digital sovereignty

To address these growing concerns and empower organizations with control over their data in the cloud, Google Cloud is guided by a three-pillar approach to digital sovereignty:

01

Data sovereignty provides customers with mechanisms to control the location of their data, prevent the provider from accessing their data, and approve access only for specific provider behaviors they deem necessary.

02

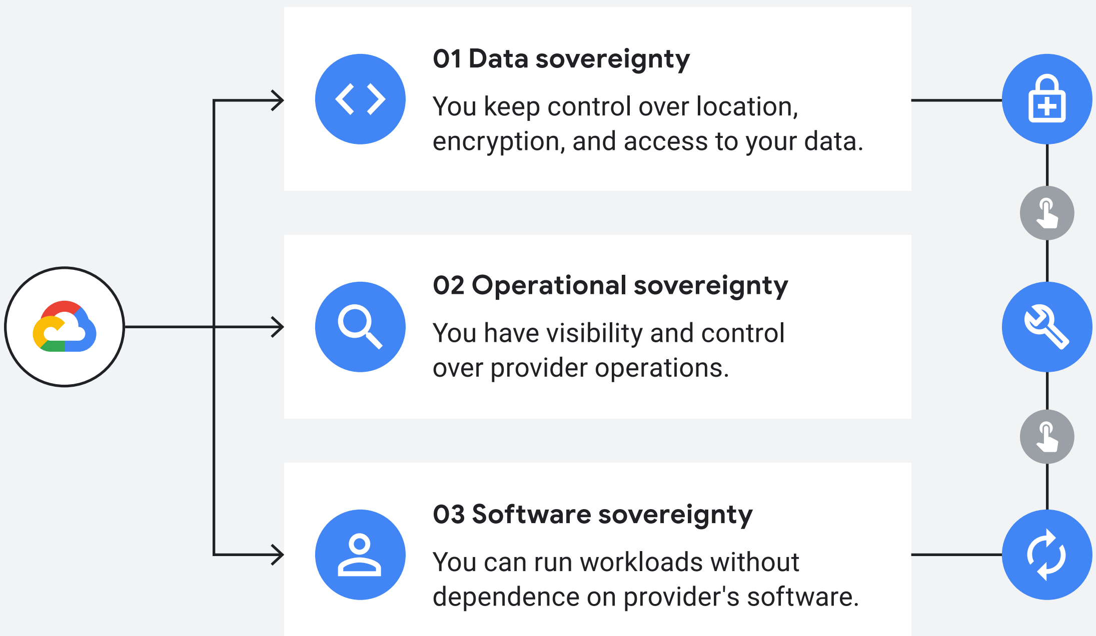
Operational sovereignty delegates the controls or the full operation of workloads to domestic partners or the customer itself. It includes controls restricting the deployment of new resources to specific provider regions and limiting support personnel access, based on predefined attributes such as citizenship, security clearance or geographic location.

03

Software sovereignty often referred to as “survivability”, provides customers with assurances that they can control the availability of their workloads and run them wherever they want, without being dependent on or locked-in to a specific cloud provider. This includes the ability to survive events that require them to quickly change where their workloads are deployed and what level of outside connection is allowed.

Google's approach to Digital Sovereignty

Our approach provides customers with comprehensive support for the three key pillars of sovereignty.



Organizations may have requirements across some or all of these areas, and their needs may evolve over time. Therefore, service providers must offer solutions addressing the depth and breadth of sovereign requirements. They must provide flexibility and choice from various technical controls to meet these needs. These solutions should also integrate seamlessly with existing business applications and technologies, and be built on a highly secure foundation, as security is paramount to achieving sovereignty.

Why choose Google Sovereign Cloud?

Google Sovereign Cloud enables governments and regulated enterprises to leverage the full power of Google Cloud, including its innovation, security, and cost-effectiveness. Google Sovereign Cloud offers the most comprehensive set of sovereign capabilities, allowing organizations to adopt the right controls on a workload-by-workload basis to meet their data, operational, and software sovereignty needs.

Partner, customer, and Google managed options

Public cloud

Run regulated workloads maintain data residency, operational oversight, and encryption management within geographic regions.

Google Distributed Cloud

Bring air-gapped configurations and other infrastructures and services for highly sensitive data to data centers and edge locations.

Google Workspace

Create and connect seamlessly with productivity and collaboration tools while maintaining control of your data.

Controls

Data residency | Access transparency & approval | Monitoring | Encryption management | Confidential compute | External key management | Client-side encryption | Physical location | Full disconnection

Google Sovereign Clouds offers:

01

Unmatched control and oversight

Google Cloud has a unique ability to deploy and scale External Key Management across its services. Unlike traditional customer managed encryption key capabilities, Google Cloud lets you encrypt data at rest with keys stored outside our infrastructure. It requires detailed justifications for each key access request. Our External Key Management offers customers or domestic partners the ability to deny access for any reason, including extraterritorial access requests. Google Cloud also delivers extensive visibility into administrative access — across more services than any other provider. We are the only major cloud provider offering customers the ability to require approval before specific administrative activity occurs, along with a mechanism for customers to ensure approvals are legitimate. These capabilities, when combined with Confidential Computing, make you the ultimate arbiter of access to your data on Google Cloud.

To address specific **data sovereignty** concerns, we enable users to enforce strict data residency by dictating the exact geographic boundaries for data storage and processing. We allow organizations to store and manage data encryption keys outside our infrastructure, outside of our control.

To address **operational sovereignty** concerns, Google Cloud is the only cloud provider with options for third-party management and oversight of critical controls in multiple EU countries. We can enable organizations to limit administrative and support personnel access, based on predefined attributes such as citizenship, clearance requirements, or residency in a particular geographic location.

To address **software sovereignty** concerns, we offer the most flexible and cost-effective air-gapped solution of any major cloud provider. Google Distributed Cloud can be deployed without connectivity to Google Cloud or the public internet, allowing for the management of infrastructure, services, APIs, and tooling in isolation. It is built to remain disconnected in perpetuity.

Google Sovereign Cloud builds on a baseline of controls and security features that offer strong protections including default encryption for data-at-rest, customer-managed encryption keys, confidential computing for data-in-use, end-user and administrative access controls and auditing, among many others.

Case studies

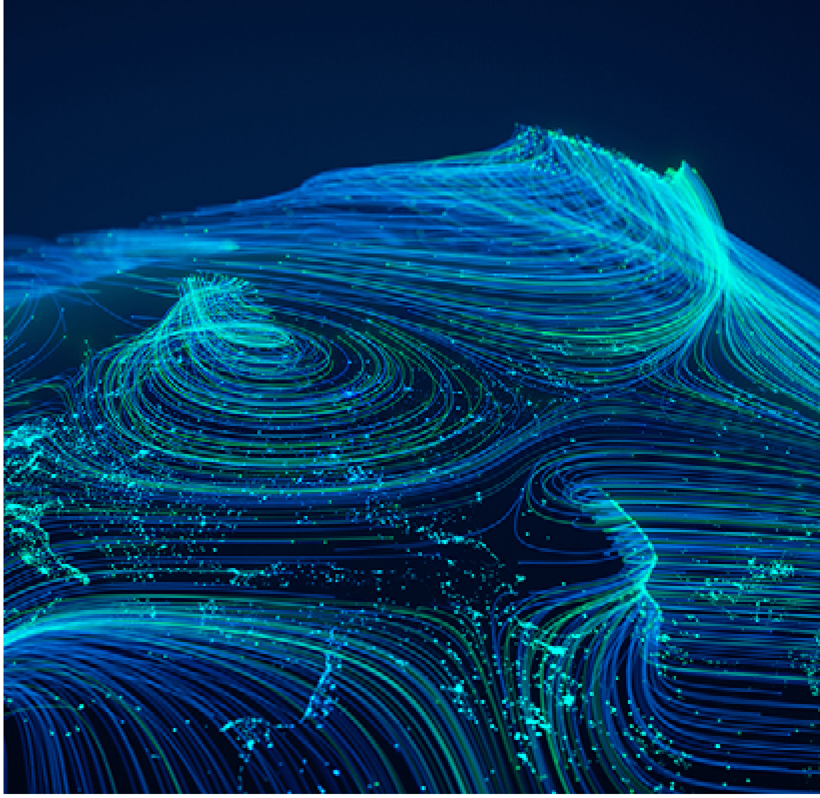
Iron Mountain, best known for their secure storage facilities, has been storing sensitive data in one way or another since it was founded in 1951. Iron Mountain leverages the adaptability of Google Sovereign Cloud's unique encryption controls to seamlessly address complex compliance regulations across 58 countries. The flexibility of Google Sovereign Cloud allows Iron Mountain to implement tailored encryption solutions to store digital and physical assets for over 225,000 customers worldwide.

The University Medical Center Schleswig-Holstein (UKSH) is the second largest university hospital in Germany, serving over half a million patients per year. UKSH will leverage Sovereign Controls by T-Systems to address data and operational sovereignty concerns as it moves to the cloud to increase their use of AI and deploy MRI imagery interpretation. It is one of several German hospitals and healthcare related organizations to take advantage of controls on Google Cloud.

Matmut is a major player in the French insurance market, with over 4.2 million customers. Matmut handles a significant amount of sensitive social data, as it accelerates its digital transformation to offer its customers a better response. Local Controls by S3NS allows Matmut to combine public cloud innovation with the latest cryptographic controls, paving the way for the adoption of "Cloud de Confiance" with the crucial SecNumCloud certification, so critical in France.

02

Global reach, local partner solutions



Many organizations express concern about foreign government access to sensitive data stored in the cloud. Others are uneasy with reliance on foreign cloud service providers to support critical national or local services and workloads. To address these concerns, we deliver capabilities that allow customers to deploy workloads with local control and assurance provided by trusted local partners without losing the transformational benefits of the cloud.

As of end of 2024, we have established local partnerships including CNTXT in Saudi Arabia, Gulf Edge in Thailand, KDDI in Japan, Minsait in Spain, Proximus in Belgium and Luxembourg, S3NS in France, T-Systems in Germany, Telecom Italia in Italy, and WWT in the US, who operate key controls such as external encryption key management and provide oversight over administrative operations or local support.

The ability to meet sovereignty requirements also requires local support for the applications customers depend on to power their businesses and drive innovation. To this end, Google Cloud has independent software vendor (ISV) initiatives — Google Cloud Ready - Sovereign Solutions and Google Cloud Ready - Distributed Cloud — dedicated to sovereign workloads.

Case studies

Clarence, a joint venture between Proximus and LuxConnect, operates Google Distributed Cloud air-gapped. The totally disconnected sovereign cloud solution is specifically designed for governments, regulated companies, and other enterprises handling highly sensitive data within the European Union. The Commission de Surveillance du Secteur Financier (CSSF), Luxembourg's financial regulatory body, has partnered with Clarence, to enable the CSSF leverage and apply Google's cutting-edge AI technology to its sensitive data, while ensuring confidentiality, complete control, and full sovereignty.

Thales, a France-based global leader indefense and security, aerospace, digital identity, and cybersecurity, aims to migrate many of its sensitive workloads to the cloud. This initiative involves modernizing their infrastructure and applications, ranging from SAP to bespoke customer solutions. Le Cloud de Confiance by S3NS enables Thales to host sensitive data and workloads in the cloud with a SecNumCloud certification.

The Centre for Strategic Infocomm Technologies (CSIT), a technical agency in the Singapore Ministry of Defence, has been collaborating with Google Cloud to tap Google Cloud's AI and data services to process high volumes of sensitive data securely in isolation from the public internet using Google Distributed Cloud air-gapped.[2]

[2] Source: https://www.csit.gov.sg/events/media-release-17nov2023

03

Data control meets collaborative freedom

Productivity platforms are the backbone of modern businesses, enabling seamless collaboration and efficient workflows. However, for organizations operating in sectors with stringent data regulations or heightened security concerns, traditional solutions may fall short of sovereignty requirements. Google Workspace is empowering these organizations to maintain strict control over their sensitive data, including its location, access, and governance, while still harnessing the full potential of productivity tools.

For **data sovereignty**, Workspace allows organizations to choose where their customer data is stored. Organizations can also choose to store a copy of their data in a specific country or locality with the local data storage capability. Workspace provides contractual assurances and technical controls, such as client-side encryption (CSE), that help prevent access to customer data from external entities, including Google and foreign government law enforcement agencies. With CSE, organizations control the encryption keys and can store them outside of Google in a physical location of their choice.

Workspace supports **operational sovereignty** through flexible key management and granular vendor access controls. Customers have the option to store encryption keys for CSE with trusted third-party providers in a chosen location or integrate their existing key management solution using our public APIs. With Assured Controls, customers can view, manage, and approve vendor actions with their confidential data.

Workspace addresses **software sovereignty** through support for open file formats (e.g. odp, pdf) and proprietary ones (e.g. Microsoft Office), allowing interoperability and collaboration across system boundaries. Public APIs based on open protocols like REST and IMAP allow integration and data flow into other systems, further helping to prevent data lock-in. In addition, Workspace is certified for SWIPO Data Portability Code of Conduct, enabling full data export on customer requests, helping organizations reduce survivability risks and avoid lock-in.

Case studies

SCHWARZ

Schwarz Group, Europe's largest and the world's fourth-largest retail group, recently signed a partnership to jointly deliver sovereign, secure workplace productivity solutions for Germany and Europe. The companies of Schwarz Group with 575,000 employees will transition to Google Workspace to maximize security, efficiency, and control of its data sovereignty.

AIRBUS

"Regionalized data processing is central to **Airbus**' compliance strategy. When data isn't regionalized or is handled by other technology providers, it's a risk for Europe, it's a risk for the nation, and it's a risk for Airbus. It's a risk that we can't afford. So, we have migrated approximately 270,000 users to regionalized data processing while maintaining the same functionality Workspace has always offered, with no reported impact to end-users, so we are able to be more productive and innovative. We control our most sensitive data with encryption keys owned by Airbus, which is only possible with client-side encryption in Google Workspace."[3]

Sebastien Aubineau,
IM Digital Workplace and Collaboration Product Leader at Airbus

[3] Source:https://workspace.google.com/blog/identity-and-security/general-availability-google-workspace-assured-controls-future-digital-sovereignty

Conclusion

Navigating the complexities of digital sovereignty requires a trusted partner. We are committed to supporting organizations on their journey towards digital sovereignty with Google Sovereign Cloud's comprehensive set of solutions. We built the capabilities of Google Sovereign Cloud for organizations with the most sensitive data and the most stringent sovereign requirements.

With our comprehensive set of controls, organizations can adopt the right controls on a workload-by-workload basis to meet their data, operational, and software sovereignty requirements, while optimizing for considerations like regional and industry-specific regulations, infrastructure platform choice, functionality, cost, infrastructure consistency, and developer experience.

To learn more, visit:
goo.gle/sovereign-cloud

Google Cloud