Location, Location, Location: The Importance of Security and Privacy of Your Data in the Cloud

Delight your customers with an Agile Cloud Experience
Overview

Data - the most valuable business asset for enterprises and their customers, must be protected from unauthorized access. Always available and secure data coupled with insightful data analytics, helps you drive business innovation, increase client satisfaction and loyalty – and more importantly, gives you a competitive edge in the marketplace. Managing data throughout its lifecycle in compliance with business, privacy and security regulatory requirements should be everyone’s top priority in cloud environments. You need a trusted business partner with deep expertise covering security, privacy and cloud deployments. IBM has successfully helped customers migrate to the cloud by using extensive industry-specific products and services backed by about 1,900 cloud technology patents granted to IBM in 2017.

The nature of global cloud computing means that the physical location of data is very relevant and is becoming more significant every day. Business transactions occur across international borders every millisecond. Big data created in one region gets stored, processed, and accessed from other regions across international borders. End users, clients, and business partners utilizing your data may be accessing it from all over the globe.

The performance of your cloud workloads is proportionate to the user distance from the data center where your data is housed. That is true for all cloud providers, who are expected to ensure your data moves efficiently with minimal latency across the globe. This customer requirement motivates IBM Cloud to invest heavily in building, maintaining, and growing an agile global cloud network backbone that transports public and private traffic across the globe with industry-leading customer experience.
Data Location Matters

Businesses often migrate their business workloads to the cloud so their data is always available and delivered quickly and reliably to customers around the world. The actual location of data is often given little attention due to lack of clarity about concepts such as universal accessibility, guaranteed uptime service level agreements, high-speed network connectivity, and more. Overlooking your data’s physical location can lead to slow uploads and downloads, unsatisfactory delays in service, a reduction in productivity, and loss of customers and business. More importantly, where data resides plays a detrimental role in protecting privacy and meeting the regulatory requirements for consumers data protection.

While the cloud delivers infrastructure as a service, data stored on the cloud resides on physical storage devices and data in transit traverse physical networks too. Even data used by your cloud applications, data in use, need to be secured too. IBM Cloud offers security solutions designed to protect data throughout its lifecycle.

When looking at the potential performance of global networks, it is customary to use the speed of light in fiber to estimate optimal potential response times as measured in return trip time (RTT).

Cloud workloads require infrastructure that is agile, secure, responsive and has a local presence on a global scale. IBM understands your business cloud needs and has invested in a global network that offers more than 60 data centers, six multizone regions, and six continents. IBM's cloud network helps to keep your application workloads and your date secure in data centers that are compliant with regulatory requirements. IBM's data security adresses data at rest, in transit and in use. It is worth noting that IBM is the only cloud provider certified with Federal Information Processing Standard (FIPS) Publication 140-2 Level 4, which is the highest possible standard for cryptographic modules, that encrypts your data to keep it private and safe.

The location of your cloud resources plays a significant role in how quickly and reliably your data can be accessed by users around the world. Downloading a 10GB file from a data center on the other side of the globe takes much longer than the same download from a closer data center. Geographic proximity plays a detrimental role in user’s experiences and their business purchase decisions.
Customer Scenario

The ideal situation for enterprises is to deploy their cloud workloads in proximity to their customers for best response time. Today's global digital economy means that most enterprises conduct business around the globe and need to ensure that customers, regardless of their location, have pleasant business experiences. For the best experience, enterprises could take advantage of IBM Cloud's global presence and deploy their workloads in several locations that are close to their global customer base.

Let's look at a global business that is based in San Jose, CA with customers in Paris, France, and Singapore. The ideal situation for the business is to have workloads deployed near San Jose, Paris, and Singapore, which is something that IBM Cloud can deliver. Alternatively, the business could choose a less optimal solution by deploying their workloads in San Jose; thus, giving customers in Paris and Singapore, almost similar response times. IBM Cloud's expansive network and multizone region capabilities, coupled with high-speed infrastructure are designed to enable businesses to serve their customers in a secured, fast and timely manner.
IBM Cloud Global Data Centers

Protection and Delivery of Services to Customers

All IBM Cloud data centers and network points of presence (PoPs) are connected to our innovated global network backbone, which carries public, private, and management traffic to and from servers. Our global network boasts more than 2,600Gbps of connectivity between data centers and network PoPs—and our network PoPs have more than 2,500Gbps of transit and peering connectivity to the Internet. When you access an IBM Cloud server, the network is designed to bring you onto our global backbone as quickly as possible at one of our network PoPs. Clients and end users may experience fewer hops (and a more direct route that IBM Cloud controls). When a user requests data from an IBM Cloud server, that data travels to the nearest network PoP where it’s handed off to another provider to carry the data the remaining distance.

Figure 1: IBM Cloud Worldwide Data Centers and Multizone Regions
When utilizing IBM Aspera on Cloud, enterprises can move files and data sets of any type and size reliably at maximum speed regardless of network conditions. IBM Aspera uses patented network-optimized proprietary protocol Fast and Secure Protocol (FASP) to move data with security and at speeds that often exceed one hundred times speeds delivered by Transmission Control Protocol (TCP). Data transfers using FASP are encrypted for securing your data at rest and in transit. This solution is designed for quickly, reliably and secured movement of large files and data sets between clouds and on-premises resources.

Deploy Workloads in Over 60 Data Centers, And Now Into 6 Regions and 18 Availability Zones

IBM Cloud is constantly expanding its global footprint to help ensure you’re meeting your customers where they are. Our IBM Cloud multizone regions (MZRs) have three or more data centers within six miles of each other. Located in proximity to help ensure high availability and resiliency, they offer a full and consistent set of services to support our clients’ enterprise-class workload needs. MZRs include the full IBM Watson and Cloud stack (IaaS, CaaS, PaaS, Cognitive, and Data), and are connected to two POPs to help provide maximum POP resiliency. High-speed metro-area interconnects allow applications to have <2ms latency in cross zone communications. IBM Cloud Services, such as cloud object storage, containers, and API and de-identify data under applicable permissions are regionally aware and take advantage of this easing burden on the application provider.
Our Responsibility to You

Data is the most valuable business asset of our time. It’s the world’s new natural resource, growing exponentially not only in quantity but more importantly, form and value. Every action and interaction, every decision and relationship, every event occurring in any of the world’s complex systems, is now expressed as data. This profound shift is compelling enterprises and enterprises to adopt new technologies and business architectures, based on cloud; and new business processes, skills, and forms of engagement. In the rush to harness potential business value from data, cloud providers mustn’t lose sight of basic expectations that individuals, enterprises, and communities rightly have regarding security, trust, privacy, jobs, skills – and, increasingly, the data they own or that is collected from them.

Data Ownership & Privacy

IBM Cloud believes that the unique insights derived from our clients’ data are their competitive advantage, and we do not share them without clients’ explicit agreement. We employ security practices to help safeguard data, including the use of encryption, access control methodologies, and proprietary consent management modules, which allow us to restrict access to authorized users.

We advocate for strong and innovative means to enhance privacy and data protection, and we will continue to invest in privacy enhancing technologies. We were an early adopter to the European Union (EU) Data Protection Code of Conduct for Cloud Service Providers for several IBM Cloud services and offering – securing certification under the U.S.-EU Privacy Offerings and the APEC Cross-Border Privacy Rules. IBM was the first cloud provider to deliver hyper data protection and commit to the EU’s General Data Protection Regulation (GDPR) compliance. IBM Cloud is GDPR compliant.

Data Flows and Access

Protecting the privacy of your data, which is fundamental in our data-driven society, is something that IBM Cloud appreciates and is fully committed to. IBM Cloud is making significant investments in our cloud data centers around the globe to give clients the flexibility to decide where to store and process their data. We believe these decisions generally should be driven by client choice rather than government mandate.

Data Security and Trust

IBM Cloud employs security practices and technologies to help safeguard workloads and data. On the IBM Cloud, data is protected while at rest, in transit and in use. We’re poised at the forefront of applying artificial intelligence capabilities to stay steps ahead of emerging digital threats. We do not put ‘backdoors’ in our products for any government agency, nor do we provide source code or encryption keys to any government agency. You are the only party that would own your encryption keys and not even IBM would have access to those keys. IBM Cloud security builds on IBM’s heritage as a time tested security company with on-the-field tested security solutions used by thousands of enterprises worldwide.
Resources

Deploy locally and scale globally. To learn more about IBM Cloud data centers, visit:
https://www.ibm.com/cloud/data-centers/

Never neglect your network. Learn how to design your cloud to boost traffic and protect your data. Learn more about IBM Cloud Network:
https://www.ibm.com/cloud/network

The data economy is evolving rapidly. Read our views on data responsibility: