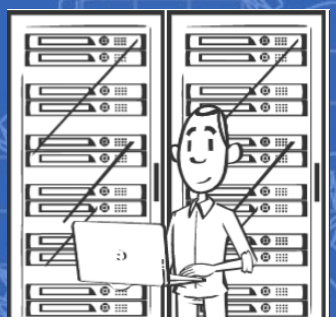
Mini Customer FAQ



Here are some of the frequently asked questions/concerns when it comes to who controls data and where data is stored.

1 Does data residency within my country provide better security?

If IT systems are in any way connected to the Internet (or other multi-party networks), even indirectly, they are at risk and susceptible to a wide range of logical access threats, regardless of the physical location. Internet connected systems expose an organization to a broad threat space, all of which are propagated from any location. With cloud technologies you can reduce security threats by:

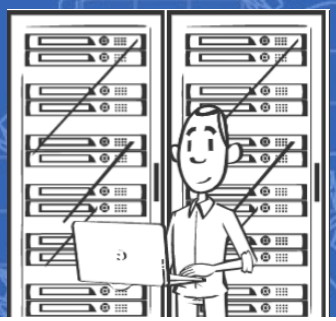
- **Automating manual processes and reducing risk of human error.** A common example is a failure to patch vulnerable systems with published software updates for many months prior to an exploit. The manual process of updating systems with the latest patches is difficult and is not feasible to do regularly without automation.

- **Increasing your control over who has access to your data.** The vast majority of major data compromises have occurred either through unintentional errors or intentional malicious behavior by individuals using authorized accounts that have made data exploitation possible. With cloud technology, you have the ability to tightly control who has access to what data and logs to see who and when data was accessed by individuals within your organization.

Both Gartner and IDC[1], two leading IT research organizations, concluded that the security posture of major CSPs is equal to or better than the best enterprise data centers, and that security should no longer be considered a primary inhibitor to the adoption of cloud services.

Footnotes:
1. Pete Lindstrom, “Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment,” International Data Corporation (July 2015)

aws



2 Does cloud increase the impact of compelled access risk?

"Compelled access risk" or "compelled disclosure" refers to access rights to data by governments or their agents under laws and regulations at the national, provincial, and sector levels in any given country. Public Sector customer are often concerned that compelled disclosure may leave a data owner with no ability to prevent access to its data by a sovereign entity purporting to invoke applicable law. However, a sovereign nation's lawful access to data is not a cloud-specific issue.

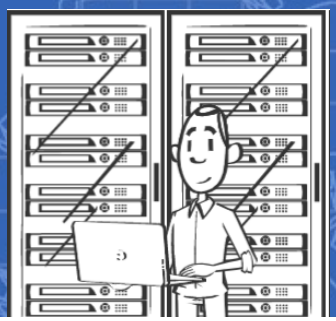
Owning the physical system, either directly or through an outsourced contract, does not reduce the risk of compelled access because there are already other legal mechanisms in place that give governments in one jurisdiction the means to request access to data stored in another jurisdiction. Compared to a traditional on-premises environment, law enforcement must generally overcome more barriers when attempting to compel a CSP to disclose another customer's data. Law enforcement cannot search or seize data stored in a CSP's servers without abiding by the legal frameworks supporting a narrowly targeted set of law enforcement purposes.

In addition, CSPs can challenge requests that are overbroad, exceed the requestor's authority, or do not fully comply with applicable law. CSPs like AWS are fully committed to providing affected customers with notice of data requests, enabling the customer to engage with authorities and/or take further appropriate action to prevent against improper disclosure of its data. This complex challenge is not unique to the U.S. government or U.S.-based companies, because any multi-national company is subject to applicable laws and regulations at the national, provincial, and sector levels in any given country regardless of the location of data.

3 Do data residency requirements have an effect on my cloud environment?

Restricting operations to specific in-country requirements inhibits service innovation and hinders the ability to compensate for threats, such as ones that target availability. Another detrimental by-product of in-country geographic constraints is that threat actors can gain targeting accuracy knowing the data must reside within specific areas. Hyperscale CSPs have available offerings and supporting architectures to offer both defense in depth (the practice of implementing multiple layers of security controls) and defense in breadth (the approach of using multidisciplinary activities to provide numerous protection mechanisms at each identified layer of defense) capabilities. This is due to security mechanisms being intrinsic to the design and operation of hyperscale CSP offerings.

Mini Customer FAQ



4 Will data residency requirements have an effect on the economic growth and workforce development opportunities that hyperscale CSPs can provide?

There can be significant negative impacts to implementing data residency requirements, such as:

- **Adverse effect on local business multi-national commercial expansion efforts:** As businesses grow and expand outside regional operations, it is vital that they have access to resources that have a global reach. Restricting access to hyperscale CSP services severely limits the level of user experience that a business can provide to its global customer base.

- **Limited geo-redundancy options compared to global CSP regions:** For governments and businesses, ensuring redundancy in the event of operational failure due to a disaster or other circumstances is vital for stability. Having clustered operations in only one country exposes the organization to a level of risk that can far outweigh data access concerns.

- **Expensive cost structures necessary to accommodate stringent requirements:** Single tenant or community built "cloud" environments require a level of pricing for operational sustainability that can actually take away from procuring the additional capabilities needed for achieving defense in depth. Cloud technology is the enabler for commercial and public sector advancements, and the extent to which governments promote or oppose the principle of cross-border data flows will impact the strength of their local economies as well as their global marketplace competitiveness.

5 If I put my data in the cloud, will I lose control of it?

In the Shared Responsibility model, the customer maintains control over their data. There are five important basic concepts regarding data ownership and management in the shared responsibility model:

1. Customers continue to own their data.
2. Customers choose the geographic location(s) in which to store their data; it does not move unless the customer decides to move it.
3. Customers can download or delete their data whenever they like.
4. Customers can "crypto-delete" their data by deleting the master encryption keys that are required to decrypt the data keys, which are, in turn, required to decrypt the data.
5. Customers should consider the sensitivity of their data and decide if and how to encrypt the data while it is in transit and at rest