BIFROST
STORAGE CLOUD

Compliance Standards Need to Catch Up

Bifrost Cloud's Security and Compliance Story

Security & Compliance Not Always Aligned

Security and compliance may always appear to be in alignment. However, there are some facets of information security where they diverge and no longer synergize. In modern IT infrastructure, the conflict between increasing security versus maintaining compliance is becoming more apparent. Compliance fails to keep pace as we push for decentralized, highly robust, and resilient information systems.

Let's explore how compliance lags behind the quickly evolving cloud computing infrastructure. Before beginning, we need to cover some basics of where these conflicts spawn.

Security Risks of Centralized vs. Distributed Architecture

The demand on businesses to maintain more terabytes of data every year forces IT Managers to find a more cost-efficient and scalable solution. These demands obsolete old infrastructure building methods, like having all your servers and data in an office closet or one data center. Cloud-based storage services are the natural solution. Instead of purchasing a new and larger capacity storage server every few years, we can expand our storage in the cloud with a few clicks. However, IT infrastructure architects can fail to consider some basic security principles when migrating into the cloud.

Relocating to one of the big three cloud providers does not distribute your data, geographically securing it. No, by default, your data is still housed in one location. This means you are still in the old paradigm of one office closet or data center housing your data. To truly secure company data, we need to distribute our data among multiple geographically diverse clouds. However, geographically diversifying where we store our data is a challenge not everyone is ready to take on.

In December 2021, many IT infrastructure architects received an involuntary audit of their AWS distributed architecture when the Northern Virginia (US-EAST-1) data center went offline. When the AWS Northern Virginia data center went offline, thousands of big and small companies dropped off the Internet. The companies could have avoided the outage if they had set up regional replication and failover. However, many did not consider the security impact of a centralized cloud environment. As a result, these companies could not conduct business for 7 hours in the middle of a Friday. Although this event only impacted network connectivity, some data center events destroy data. Take, for example, the fire suppression test that generated a high-frequency sound wave that destroyed hard drives in a Swedish Data Center in 2018. Data destruction events like the one in the Swedish Data Center are not one-offs and prove there are many unexpected ways data is destroyed in a centralized cloud.

The centralized cloud's security risks are clear, and the solution is to use a geographically distributed cloud architecture. Building a distributed cloud to house your data is not something every company's IT Department can take on. Bifrost solves this issue for you. Our Distributed Cloud Architecture has scaled out to include 20,000+ geographically diverse storage providers, from which, we select the best 80 for the specific object stored.. The result is a data storage system with unparalleled resiliency. The Bifrost network would need to lose more than 50 storage providers simultaneously for data loss to occur. In a security risk matrix, this risk is so low as to be non-existent.

Compliance's Obsolete Data Residence Requirements

After weighing the security risks, our data's need for distributed cloud architecture is evident. However, several compliance frameworks have not caught up with this ideology. The primary point of conflict between security and compliance is over data residency.

Data residency requires that all customer data be processed and stored in an IT system that must remain within a specific country's borders. Data residency is one of the foremost concerns for governments that want to use commercial cloud services. Concerns about other government requests for data, third-party unauthorized access, and general cybersecurity issues have contributed to the ongoing emphasis on keeping data within national boundaries. Some governments have gone so far as to insist that mandating data residency provides an additional layer of security. However, once you understand the underlying distributed storage architecture, these concerns are moot points.

In Bifrost's distributed storage architecture, if you wanted one file from the data storage, you would need to collect 30 different pieces to rebuild the original file. Bifrost's distributed storage works by using erasure coding to break up files into 80 chunks and distributing those 80 chunks among the 20,000 storage providers availables. So if a government decided to raid a storage provider to take your data, they would need to pin point at least 30 storage providers hosting your data to reconstruct it. If that is not enough, add that the data is AES-256 encrypted. For reference, cracking and decrypting AES-256 would take about 2.29*10^32 years; good luck with that. Through erasure coding and military-grade encryption, is the one piece of data in a data center even actual data at that point? No, it's not; it's just a binary blob of gibberish. For these reasons, data residency is no longer a security risk with a security-focused distributed storage architecture design like Bifrost's.

Instead of focusing on data residency, compliance frameworks need to focus on data assembly or access points. That is to say, where are the 30 pieces reassembled, decrypted, and accessed? The data assembly point should be the security focus and geographically restricted, not where the binary blobs of gibberish are stored. However, some companies must abide by their restrictions until compliance frameworks have caught up with the modern distributed cloud. Bifrost has you covered here too. We can offer data geofencing, keeping all your data within a specific national border. While data geofencing does not make sense from a security perspective, we understand that companies may be required to jump through arbitrary hoops.

Physical & Operational Security

Another point of conflict between security and compliance is the physical and operational security of the storage hardware itself. Many standards still include detailed requirements around the physical security, operational process, and training of the storage provider's facility, hardware, and team. In a solution with a true zero-trust architecture, these become irrelevant as well. No one storage provider is capable of accessing or manipulating the data object in any way. Even if there is a failure and the physical hard drive is lost, the net effect on the data object is zero. The object is still as secure and recoverable as ever. This especially holds true if the end to end encryption (E2EE) option is utilized.

Wrapping-Up

Policies must evolve to reflect the changing realities of technology and modern distributed storage architectures. Otherwise, governments and businesses will fail to modernize their operations and implement the most modern and secure solutions. Moreover, imposing data residency requirements can hinder a company's growth in new markets. Data residency requirements force businesses that want to do business within a country to follow and build segmented infrastructure for that country's data. That adds costs for more infrastructure, personnel to manage the infrastructure, and an internal compliance team to circumnavigate the legal requirements. Data residency is an additional burden without any added security. So it is time to rethink the value of data residency and modernize compliance requirements to match the reality of distributed cloud architectures.

About Bifrost Cloud

Founded in 2019 out of Toronto, Bifrost Cloud is a leader introducing distributed cloud storage to the B2B marketplace. With simple and competitive pricing, S3 API, a generous SLA, and exceptional customer service, they have removed the barriers that have prevented traditional IT from embracing this next-gen technology and are currently looking for reseller partners.

Bifrostcloud.com

Works Cited

1) Amazon.com: AWS Service Event in the Northern Virginia (US-EAST-1) Region
2) TheRegister.com: Nordic Nasdaq knocked as deleterious decibels crashed servers
3) UbiqSecurity.com: 128 or 256 bit Encryption