Meeting Data Security Demands With Object Storage

by Joseph Ortiz, Senior Analyst

Data is the lifeblood of every organization. An organization's data comprises important information such as customer and financial records, internal processes, marketing tactics and strategies, details of products and/or services that it produces. All of this contributes to an organization's ability to conduct day-to-day business, compete successfully in the marketplace and provide a competitive advantage. Data is key to an organization's success; it is your treasure, history, unique competitive advantage, customer relationships, etc. Consequently, it is in your organization's best interests to ensure that its data is protected against potential loss or unauthorized access.

The Rising Data Flood

Organizations today are dealing with managing and storing ever-increasing amounts of data for increasing periods of time. Why are businesses storing more data and for longer? This situation is the result of a variety of factors such as:

- Data as the currency of business
- Business analytics that can monetize existing data stores in new ways to produce additional profit and business intelligence
- The growth of mobile applications tied to data center resources
- Large quantities of unstructured data from new devices such as sensors, video cameras and other Internet of Things (IoT) sources

Given the ever-increasing amount of business data, it is clear traditional storage systems aren't up to the task. What's needed are advanced storage systems that can scale to an almost unlimited amount of data while providing for its security, organization, management, and protection.

Why is protecting data more critical than ever? It is essential for an organization to secure data and protect its availability for several reasons:

- Today's business landscape no longer operates on a 9 to 5 basis, five days a week.
- Business operations, especially eBusiness, are now open 24/7, including holidays.
- Data is a competitive asset; each scrap might lead to new opportunities.
- To meet any legal requests from courts or governmental agencies in a timely manner.
- To protect the organization against legal challenges from other entities or litigation for current or past employees and customers.

Commissioned by HGST, a Western Digital brand

Modern object-based storage (OBS) systems should be a consideration for organizations looking to address these security and data protection issues. Unlike traditional solutions, an OBS system is vastly more scalable and simpler to manage. Rather than organizing files in a directory hierarchy, OBS has flat organization of containers, also called buckets in Amazon S3, and use unique IDs or keys to retrieve the objects.

Threats to Data Integrity

A primary concern is protecting data integrity, which means assuring the accuracy and consistency of data throughout its entire life cycle. It is critical to ensure the accuracy and quality of the objects (files) written to the storage media. There are a number of events that can threaten data integrity and availability. A common threat is hardware failures or malfunctions that can destroy or corrupt data.

Modern OBS solutions have various advanced features, such as Rateless Erasure Coding, that can mitigate the challenge of restoring the data on failed hardware far more rapidly than RAID implementations. With the ever larger size of hard drives, RAID-based data protection schemes have to operate in a degraded condition during a volume rebuild for much longer times than in the past. This dramatically increases the likelihood of an unrecoverable data error. This is in sharp contrast with erasure coded environments where there are is no rebuild time in the case of hardware failure.

Other advanced data protection methods include continuous monitoring and data integrity checking of every object and performing automated self-healing in the event it finds anomalies. This helps ensure the integrity of the data on these systems.

Traditionally an additional layer of data protection has been provided by generating redundant copies of the data through regularly scheduled backups, snapshots and the replication of the data to different media in different locations. However, with an erasure coded environment of say 18/5, up to five data shards can be inaccessible without losing object availability. In a three geo-distributed configuration with erasure encoding of 18/8, a major Disaster Recovery (DR) event where an entire server or even a data center becomes inaccessible will not cause the loss of data availability. Even if a redundant cold copy is still deemed necessary, a distributed OBS solution with erasure coding can reduce the amount of storage the organization needs to protect its data.

Ensuring Data Security

While data integrity and availability are important, another threat is data access by unauthorized persons who could misuse, modify or even destroy the data. Whether the data is at rest on a storage device or in transit to a different device or system, it is at risk from unauthorized access if not properly secured. Hence, it is not sufficient to ensure only integrity and availability, data security is paramount for business success.

Unauthorized access to a business' data can be extremely damaging. For instance, if unauthorized persons were able to access or intercept the financial records of a publicly traded company, they could use that information to take advantage of this insider information and share it with others in order to make an illegal profit.

Another example would be unauthorized persons accessing a business's marketing information and plans then revealing or selling that information to competitors. This would give the competitors an unfair advantage that would be damaging to the organization. This is why properly securing its data is so important for a business.

Ensuring proper data security requires two main components, secure access control and proper data encryption utilizing industry accepted protocols and methods.

The first line of defense for data is robust, 256-bit AES encryption combined with encryption of data at rest keeps the information protected against access even if an individual was able to surreptitiously copy an object.

Data should be encrypted whether it is at rest or in transit to another device or system. Encryption should be selectively available at the business functional level (bucket or container) as opposed to technological level (hard drive). This provides the flexibility of supporting multi-tenancy with different encryption keys for each data set, making it an ideal solution for service providers or enterprises looking to be more service oriented with their IT resources. Thus, even if an unauthorized person intercepts or acquires the encrypted data, it will be useless without the proper keys to decode it. Any object storage system under consideration by an organization should provide these encryption capabilities.

The second line of defense is provided by the organization's system security protocols and settings that define the access rights and levels for individual users and groups. Best practices include a well-defined password protocol with strong passphrases as well as regular rotation and mandated waiting period for passphrase reuse.

Conclusion

We strongly advise organizations to carefully consider the value derived from their data and how this contributes to their business success. They should pay close attention to how they store, protect and analyze data. The loss of any data can have a significant negative impact on an organization’s ability to conduct business and ultimately its financial success. Further, data loss can expose the organization to expensive liabilities for failing to meet various compliance mandates. Additionally, failure to properly safeguard data from can result in data being stolen, modified or even destroyed, as well as being relayed to other unauthorized parties to the detriment of the business.

A modern OBS solution offers organizations the ability to scale their storage literally to the cloud while cost-effectively protecting data availability and guarding against data corruption and unauthorized access. The combination of bucket-level encryption, rateless erasure coding, and geographic distribution enable a secured, scalable storage solution for most any enterprise.

Given the potential expensive losses an organization could sustain from data loss or unauthorized access, organizations should carefully consider storage systems that provide the advanced storage, management and protection capabilities it needs to properly protect data to ensure their continued business and financial success.

Commissioned by HGST, a Western Digital brand