wasabi
hot cloud storage

Object Lock Feature Spotlight

What is Object Lock?

Object Lock is a data protection feature wherein a user can designate certain files or "objects" to be immutable, meaning they cannot be altered or deleted by anyone. Via the policies of data management applications, users set an allotted time for an object to be immutable, after which it can be altered or deleted.

Challenges with protecting data

Many organizations still view cloud storage as less secure than air gapped, offline storage. These organizations feel that if data is connected to a network, it can be accidentally deleted or susceptible to ransomware. The traditional method of air gapping data for protection meant that an organization's data was stored offline in an LTO tape cartridge or HDD that was disconnected from power sources. Retrieving data stored in this fashion could take many hours to days and is vulnerable to bit rot or damage that could ultimately destroy the data. Object Lock removes the perceived vulnerability of errant deletion or ransomware while keeping the integrity of the data, and having the data readily available and instantly accessible.

Benefits

- **Customizable immutability at the object level**
- **Support for Governance and Compliance modes**
- **Combat ransomware and viruses**
- **Avoid accidental data erasure**
- **Ensure regulatory compliance**

Why does Object Lock matter?

Because things change - especially staff. Using immutable objects ensures that information is immune from accidental or intentional deletion and alteration. It guarantees that once the information lands in the Wasabi hot storage cloud, it will remain there until the lock expires.

Because cybercriminals attack backups and archives as part of their ransomware campaigns. It isn't enough that they're taking down the primary systems, but they're also attacking the secondary/backup systems to ensure they get their ransom…

Because regulators check these things, all the time. It's essential that data in regulated industries be safeguarded for compliance and consumer protection standards.

Because legal proceedings depend on a chain of custody and immutability when it comes to digital evidence, like surveillance video, now that deep fakes and altered footage have become a threat to justice.

Object Lock can help organizations with certain government and industry regulations like HIPAA, FINRA, and CJIS for securing and preserving electronic records, transaction data, and activity logs.

Compliance Mode & Governance Mode

Wasabi Object Lock is available in two retention modes:

- Compliance mode
- Governance mode

With compliance mode, a protected file or object can't be overwritten by any user or Wasabi engineer. When an object is locked in compliance mode, its retention date can't be shortened. Immutable objects in Compliance mode will remain immutable until the end of their retention period.

With governance mode, only users with special permission, such as the root user in the account can reduce the retention settings. This allows you to grant special permission to some users if necessary.

Both retention modes allow users to place a legal hold on specific objects. The legal hold prevents a locked object from being overwritten or deleted once the original retention date has been reached. Legal holds on objects can be lifted by an authorized user. The object will remain protected until the retention period expires.

For this reason, we recommend that users only store data in compliance mode that they are certain will not need to be changed.

Object Lock and Bucket Immutability: Two Options for Data Protection

To set Object Lock permissions you must first create a new bucket with Object Lock enabled. You can not add Object Lock capabilities to an existing bucket. In an Object Lock-enabled bucket, retention periods can be set at the object level for each individual object. Alternatively, buckets can be configured to allow for a default retention setting for all objects that are placed in them. For example, if the bucket level policy is set to retain an object for 30 days, the 30 day retention is calculated and applied as each object is added. Therefore, users do not have to set each object's retention individually.

Wasabi also supports immutable buckets. In an immutable bucket, all objects are made immutable according to a uniform set of parameters. All of the objects in the bucket share the same expiration date. There can be no variation in the retention period between individual objects. This form of data protection is a great fit for protecting archival data or primary data that may not have additional copies.

Both Object Lock and immutable buckets prevent the most common causes of data loss and tampering. Helping users:

- Combat ransomware and viruses
- Avoid accidental data erasure
- Ensure regulatory compliance
- Mitigate financial risks and legal exposure

Use object immutability for greater control over individual object retention rates, and use bucket immutability for protecting large swaths of data.