FAST LTA
We secure Petabytes.

Background

Immutable Storage

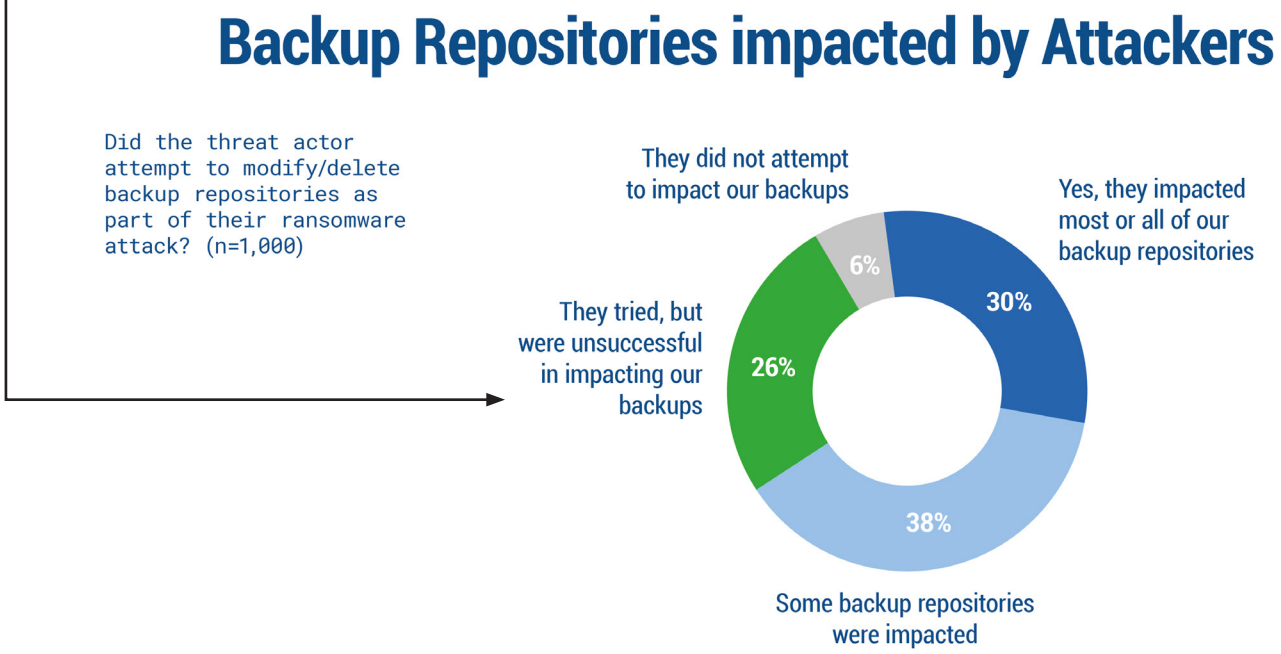
**The rise of cyber attacks demands stronger protection of data and backups. This is why immutable storage is becoming increasingly popular.
But immutability is nothing new at all. For those who remember, it was already possible to prevent overwriting of audio cassettes by breaking out a tab on the top. What is new about immutability is its use in the area of object storage, where data is write-protected for a certain period of time by so-called object locking. However, automatic snapshots, WORM sealing and Air Gap are also methods of storing data "immutably" and thus protecting it from unintentional or unauthorized deletion or manipulation. So what matters?**

Audio cassettes had a mechanical „immutability"
mode: by breaking out a tab on the top,
overwriting was no longer possible.

August 2022

Backups are particularly at risk

Backups are the prefered choice to protect your company against the consequences of cyber attacks such as ransomware. Nevertheless, it is now no longer enough to rely solely on a proven backup strategy based on the 3-2-1 approach. According to a study published by Veeam, over 90% of cyber attacks now target backups. Almost 70% of the attacks are successful: they succeed in encrypting backups completely or partially and thus rendering them unusable. Only just under a quarter of attacks could be completely prevented. Veeam comments as follows: "**This is why immutability and air gap matters.**"



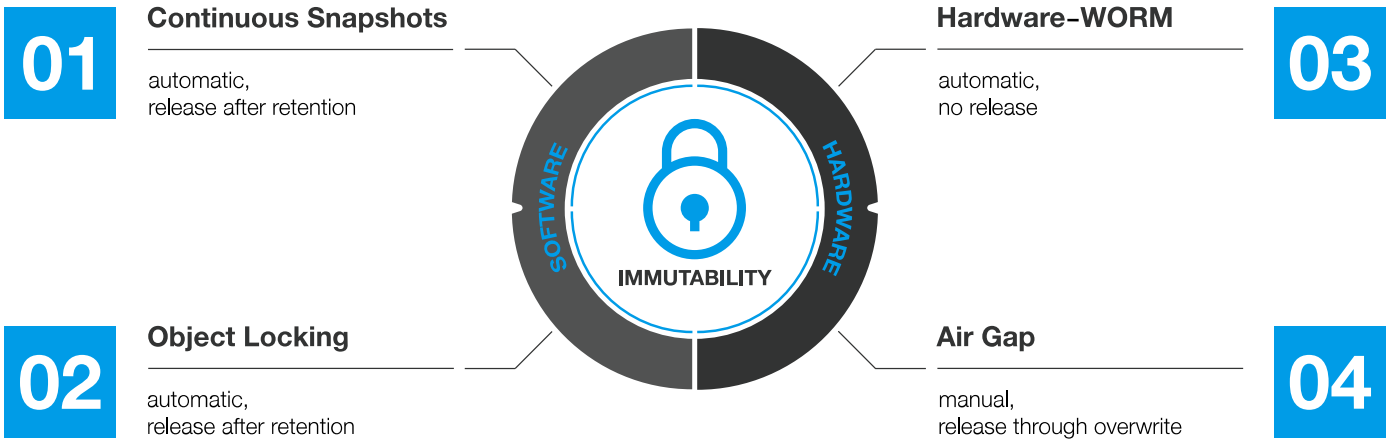
94% of cyber attacks were (also) targeted against backups. 68% of the attacks were thus (at least partially) successful.

Source: Veeam

Immutability

Literally, immutability refers to the unchangeability of an object. Once created, data can neither be changed nor deleted. However, this does not have to be achieved by low-level write protection, as is the case with real hardware WORM, for example, but can be accomplished by various methods. Common to all methods is: **“Immutable” data cannot be manipulated or deleted by attackers, whether physically or programmatically - or simply cannot be accessed.**

The following methods can be distinguished, each of which can be used accordingly at different points of the data protection, also in combination.



Automatic Snapshots and S3 Object Locking:

Soft(ware) WORM

WORM – Write Once Read Many – describes the protection of an object, a file, a directory or a data storage against deletion. There are several ways to implement this protection. Simple, but not really secure, is to protect a file via the “read only” flag. **Depending on the rights management, users can easily remove this protection;** admin users can do the same. A pure “read only” designation is therefore rather unsuitable for protection against attacks. Nevertheless, all software WORM protection methods are based upon a similar principle.

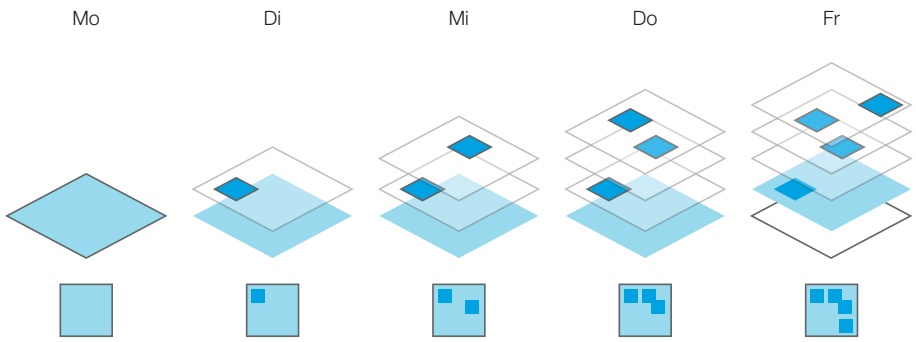
This functionality becomes a real protection through two decisive changes: First, objects are **automatically protected by the system’s logic** in the event of desired “immutability” (such as with automatic snapshots or with object locking), so they cannot be deleted by the users or admins present in the system. Secondly, a “**retention period**” is introduced, after which the protection can be removed or automatically expires.

01

Continuous Snapshots

automatic,
release after retention

Continuous snapshots work like a time machine. With each snapshot (here: daily, retention: 5d) the changes to the previous snapshot are saved. If necessary, you can restore any state saved in a snapshot.



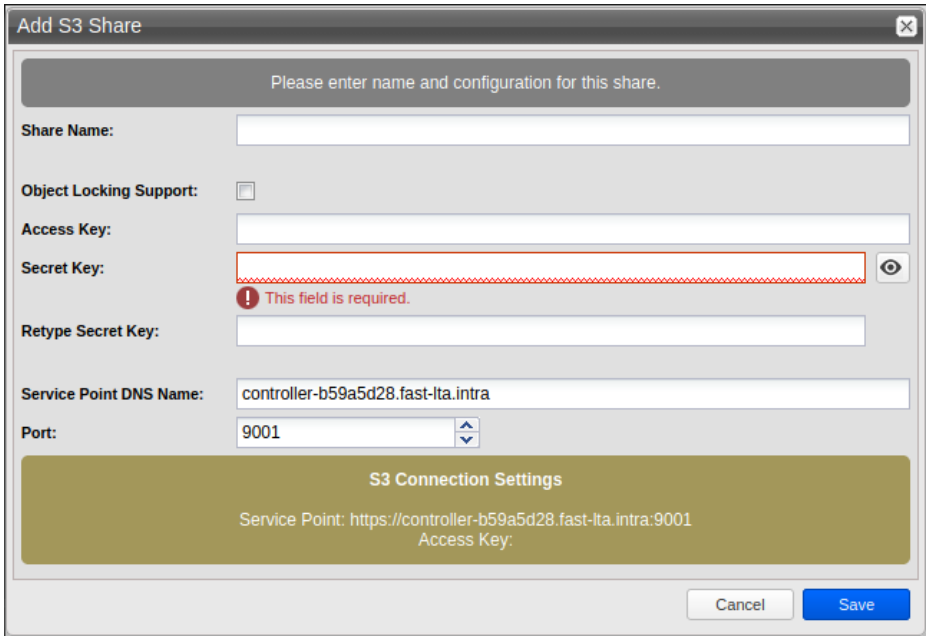
FAST LTA
We secure Petabytes.

The fundamental difference between **automatic snapshots** with retention and **object locking** with retention is the timing and control of the protection. Automatic snapshots are controlled by the storage system and create **new images of the storage state** when changes are made (including deletions), which of course require additional storage space. This makes it possible to jump back in time, so to speak, and - for a certain period of time - to granularly undo every change to the data. This makes all the more sense the "closer" the storage is to the data creation and use, since data is still more frequently (intentionally) changed or deleted there. For more distant instances of data protection, where data is rarely or never changed and should not or must not be deleted at all, **object storage** is often used, which by their very nature already requires considerably less storage space, since after an initial image only changes (incrementals) are saved. Object stores have the additional advantage that they are generally less expensive and basically infinitely scalable. **Object locking is controlled by the backup software and protects the written objects directly**: Modification or deletion is simply not possible within the retention. After the retention has expired, however, the backup software automatically ensures that the corresponding objects are deleted directly, now without object locking. **This immediately frees up storage space.**

Both methods offer high security against most attacks and manipulation attempts. Nevertheless, this "WORM" sealing is based purely on software - and is therefore potentially vulnerable to attacks. The protection of rights and accounts is in the hands of humans, which does not rule out errors and the associated security vulnerabilities. The use of two- or **multi-factor authentication** (2FA or MFA) at every relevant point is recommended to prevent unauthorized access.

02 Object Locking

automatic,
release after retention



For S3 shares, support for object locking can be optionally enabled in Silent Bricks since software version 2.45. Buckets can then be provided with retention and immutability (by the managing software, e.g. Veeam).

Hardware WORM

Protection via hardware goes much further. Here, the firmware of the hardware determines which areas of the data storage can be accessed for writing and which can only be accessed for reading. This is implemented, for example, in the Silent Cube and Silent Brick WORM by means of a “water level”: If data is written to a connected data carrier, this “water level” rises. Below the mark, the hardware only executes read commands. **Anchoring this functionality in the firmware rules out manipulation.** However, this means that the storage always requires more capacity, since individual data can never be deleted again - resetting or reducing the “water level” is simply not available in the hardware’s command set. However, security is maximized here, which is why hardware WORM is most often used for data that no longer changes or changes only rarely, such as in archiving.

Another form of hardware WORM is a physical lock, such as **breaking the tab on audio cassettes** or the switch on SD memory cards. However, since these physical locks only occur with removable media such as tapes, which require manual intervention anyway, and are also very easy to undo, they must be considered **more of a protection against user error**. If an attacker has physical access to removable media, the write protection can simply be removed again.

Hardware-WORM

automatic,
no release

03

Silent Bricks are also available with hardware WORM sealing (left: Silent Brick DS WORM, right: Silent Brick WORM). The Silent Brick and Silent Brick WORM mobile data containers are also fully Air-Gap capable.

Air Gap

Speaking of removable media: A type of “physical WORM” is the air gap, i.e. the **physical separation of media from the storage system**, as is possible with tape or **Silent Bricks**, for example. Anything that no longer has a connection to a system is protected by definition - but of course cannot be read either. For data access, the corresponding medium must first be reinserted into the system, which then also allows write or delete access again – if not additionally protected by other methods.

However, “Air Gap” is sometimes interpreted quite liberally. For example, Veeam also counts the copying or **outsourcing of data** to a separate data center (second location) or to cloud providers as an air gap, regardless of whether and how the data is protected there. To effectively protect backup data against manipulation or deletion here as well, data on object storage is secured with object locking, closing the circle again.

FAST LTA
We secure Petabytes.

Air Gap

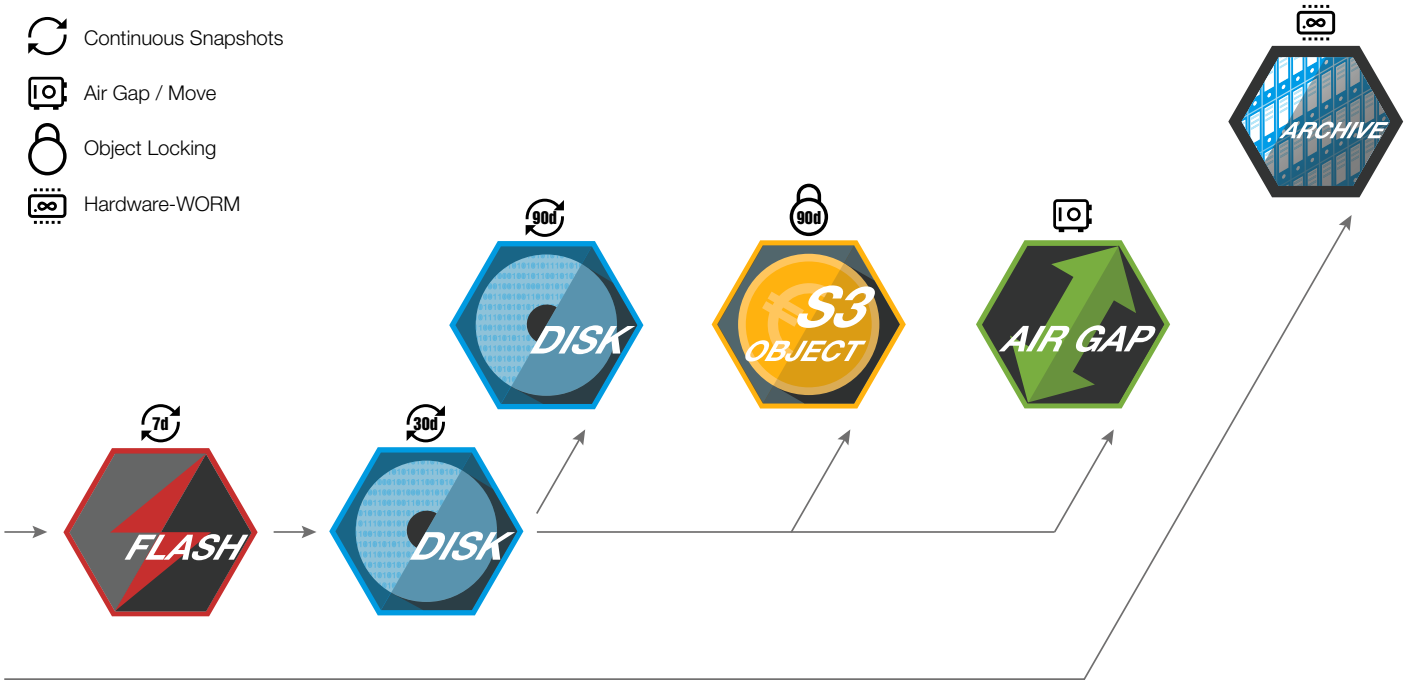
manual,
release through overwrite

04

What do you need?

Obviously, the answer is: **it depends**. As is so often the case, there is no longer one technology that covers every application. If data is to be stored long-term and 100% securely, e.g. for legally compliant archiving, there is hardly any way around hardware WORM. But for backup & recovery, it is usually not practical to store data “forever” and thus disproportionately increase capacity requirements.

Depending on the system used and the connection, all technologies are used, from automatic snapshots to Air Gap and S3 Object Locking. If physical Air Gap is not desired or not practicable due to the amount of data, data can be stored on local or remote object storage. However, these should then also be made “immutable” by the use of object locking.



Multi-Immutable Storage:

The Silent Brick System

The Silent Brick System protects data from manipulation and unintentional deletion in many ways.

In the file system (SecureNAS), Continuous Snapshots ensure that new versions are automatically created when changes are made. Like a time machine, versions up to 90 days old can be restored in an emergency.

When used as S3-compatible object storage, data can be protected via object locking and retention.

Silent Bricks offer up to 24 TB gross capacity and, as a transportable storage medium, are physically air-gap-capable, regardless of the selected protocol – even S3 buckets can be “air-gapped”.

In addition, all data that must not be lost or deleted under any circumstances ends up on the Silent Brick WORM with hardware sealing.

The individual technologies can be combined depending on the application, desired protection level and requirements. In this way, data is effectively protected against manipulation and unintentional deletion throughout the entire storage chain.

The Silent Brick System thus offers the most comprehensive “immutability” protection of any secondary storage system.

Silent Brick Controller with 2x Silent Brick and 1x Silent Brick WORM, Silent Brick DS WORM below

Silent Brick (offline)

FAST LTA
We secure Petabytes.

PROUDLY MADE IN EUROPE

FAST LTA | Ruedesheimer Str. 11 | 80686 Munich, Germany | info@fast-lta.com | **www.fast-lta.com**