FAST LTA
We secure Petabytes.

Background

Backup-to-Disk: The core element of modern data protection

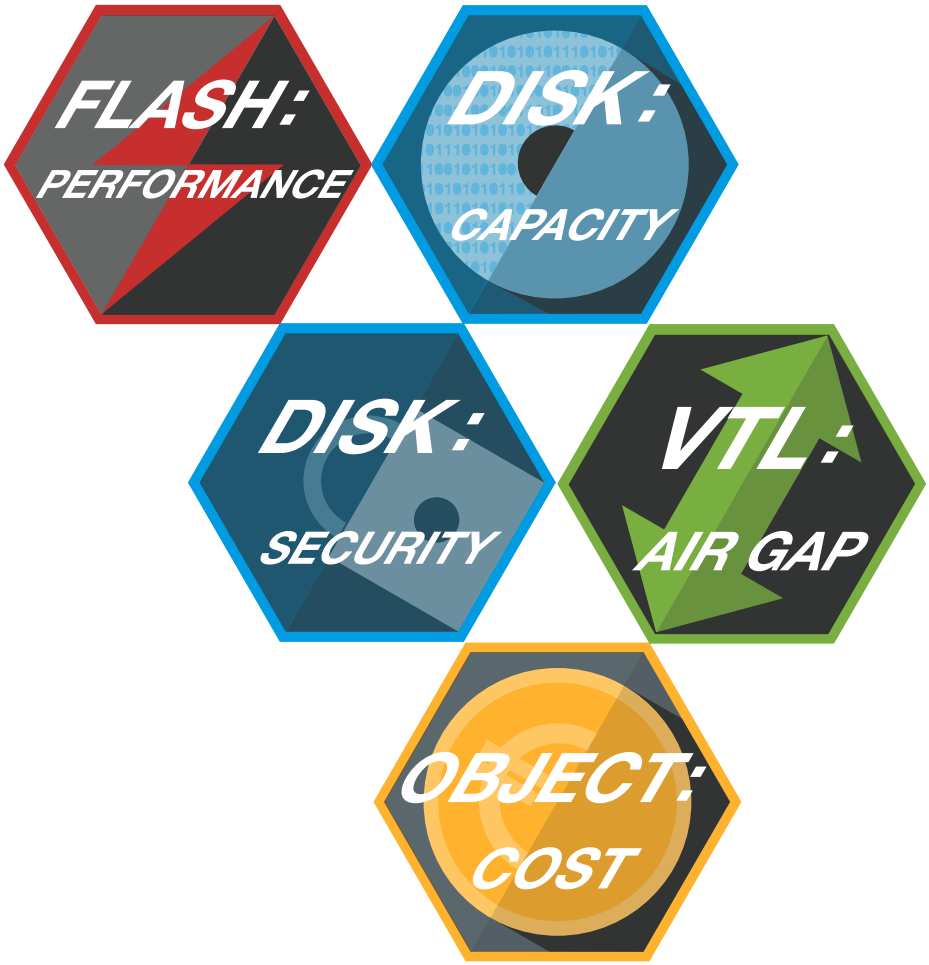
The Silent Brick is a (re-) movable data container for the Silent Brick System that contains 12 hard disks.

Various technologies used for data backup have already been declared „dead“ several times. In addition to the perennial favorite – tape – hard disks have also been repeatedly slammed. Flash storage would replace everything, and disk backups would be a thing of the past.The reality is different: Disk backups are gaining in importance. In fact, they are helping to reduce the cost and effort of flash storage and „last line of defense“ technologies.

April 2022

The new complexity of data protection

Due to the increased threat of ransomware and cyber attacks, the focus has shifted from pure backup (i.e. protection) to data protection with fast and securely functioning recovery. Instead of pure backup for the „worst case scenario“, RTO and RPO, i.e. parameters for recovering the data, are now decisive. In order to optimize these parameters, it is necessary to expand the backup strategy at both the „near“ and the „far“ end of the storage chain by means of additional technologies. This increases the complexity in the storage area. In addition to classic backup-to-disk, backup-to-flash ensures that modern technologies such as Continuous Data Protection (CDP), Forever Incrementals and InstantRecovery® can contribute to low RTO. With ever-increasing data volumes and the high load of restoring from incrementals only, flash storage systems have become indispensable here. Backup-to-(Virtual)-Tape is also experiencing an unexpected surge, albeit under a new name: Air Gap. Media that can be physically removed from the system are considered a miracle weapon against the consequences of a ransomware attack, as they are 100% protected against manipulative access. And online storage, in which data can be additionally protected by immutability, is intended for the inexpensive storage of large amounts of data, such as backup archives.



FAST LTA
We secure Petabytes.

Air Gap is often equated with tape - but with Silent Bricks there are more modern, offline-capable data containers based on disk or SSD.

Do not rely on Air Gap and immutability alone

There are various technologies for protecting data from unauthorized access and thus from manipulation. The best known is Air Gap, which is often equated with tape, but basically works with transportable data carriers - such as the Silent Brick. However, for Air Gap to actually provide 100% protection, these media must actually be disconnected or removed from the storage system. Adding them to the storage system again must only be done manually, i.e. not automatically, because the basic rule is that any automated access can be compromised. However, due to constantly increasing data volumes and “zero admin” approaches, it is desirable to reduce manual intervention as much as possible, which runs counter to the principle of frequent air-gap copying. In the case of tape archives, the problem is compounded by the fact that access can only be purely linear. Restoring individual data sets is not practical.

Meanwhile, the principle of immutability on a remote server “in the cloud” is also considered a worthwhile alternative to the Air Gap. However, this poses a problem especially in the event of a ransomware attack: the first and most important measure in such a case is to completely disconnect internal IT systems from the Internet. This means that access is only possible again once the internal systems have been 100% cleaned up - and once it has been ensured that the remote backups will not cause problems again when they are restored. Although “Storage as a Service” is considered inexpensive, restoring large amounts of data can not only take a lot of time, but can also be quite costly. In the case of online archives, the bulk of the costs are usually incurred during retrieval, and the faster the data needs to be available, the higher the costs. In addition, with software-based protection mechanisms such as “immutability,” there is always a residual risk. Any protective measure that can be overridden by special rights is not 100% secure in principle.

The term „immutability“ originates from programming, where „immutable data“ represent unchangeable values. One of the most important features of these „constants“ is the possibility of linking to them instead of having to create copies (or new instances) because they can never change. In data storage, immutability is often equated with „object lock“, a software function of the S3 protocol for temporarily locking data objects against modification or deletion. There are several levels of object lock, some of which can only be removed by adhering to the „four-eyes principle“. More information on object locking in the Backblaze blog unter https://www.backblaze.com/blog/five-ways-to-use-object-lock-immutability/

Silent Cube (left) and Silent Cube DS (right) are special systems for (compliant) archiving with hardware WORM sealing.

In contrast, a hardware-sealed WORM archive is actually completely secure. However, the separation of operational data and data to be archived should take place before the backup process. Reducing the amount of data to be backed up, shortening the backup window and the highly secure design of such an archive actually increase security. In principle, the principles of the GDPR-compliant must be observed for immutable storage in order to comply with any overriding “right to erasure”.

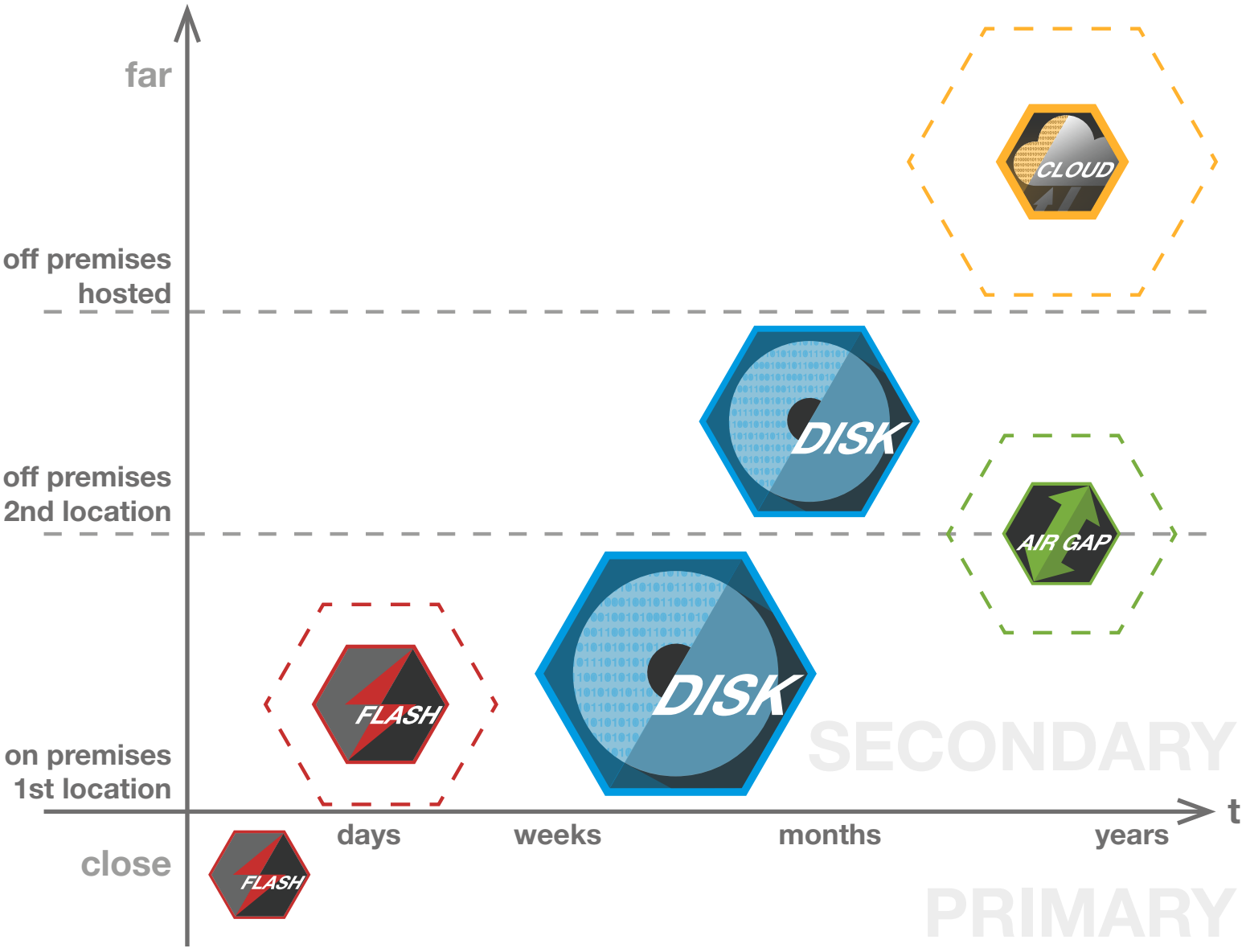
Nevertheless, these technologies are not considered the “last line of defense” for nothing, i.e. the very last option for recovering previously lost or inaccessible data. Since IT downtime is the biggest cost in a ransomware attack, these limited-access archives do little to mitigate the consequences of such an attack. In fact, they should only be seen as a last resort when all other data has been lost.

The core: Backup-to-Disk

Disk backups have proven their worth for decades as a means of quickly backing up data and providing fast, random access to backed-up data. Due to rapidly increasing data volumes, traditional RAID storage is no longer sufficient because it scales poorly and is prone to correlated failures due to the use of large quantities of the same disks. Modern disk arrays must be scalable almost indefinitely without the need for changes to the configuration (scale up). However, the reduction of the costly last instance (air gap / online archive) can only be achieved if comprehensive measures are taken during disk backup to protect against failure and attacks.

This is because the threat of targeted attacks, which first spy on the IT infrastructure - often over a period of months - and then try to make backups inaccessible, is becoming ever stronger. Should this succeed, the “last line of defense” must actually take effect - with corresponding losses in the up-to-dateness of the data and the speed of the recovery.

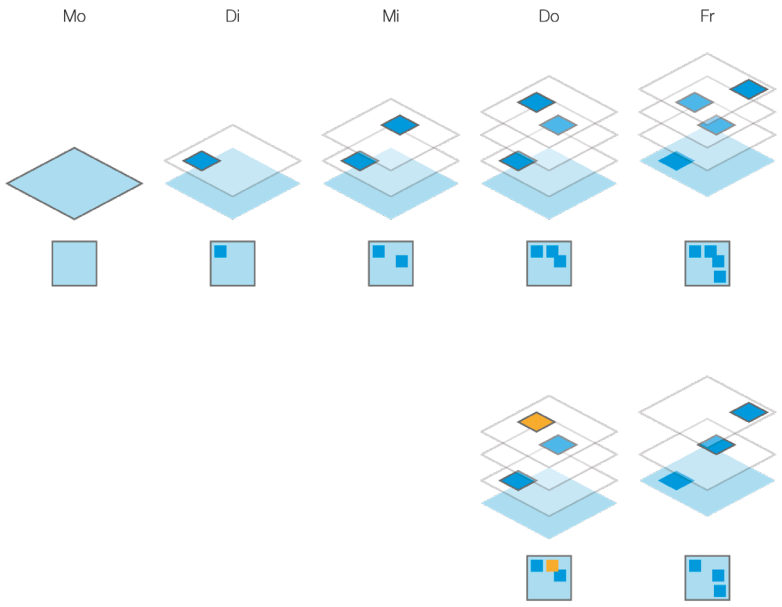
To not let that happen, there are several measures to protect the disk backup.



Disk backups are the core element of data protection. With a correspondingly high level of security, both expensive flash storage and complex air-gap technologies can be reduced.

1. Zero Trust

Too often, normal network admins or “bosses” have access to backup servers, usually through integration with standard authentication via Active Directory (AD). This represents the most obvious security vulnerability. NAS storage for backups must not be mounted directly as drives, but only via protected UNC paths. Access to all backup machines must not be via AD, but protected via multi-factor authentication. As a matter of principle, the enforcement of the “Zero Trust” approach is recommended to avoid attacks by hijacked accounts (or malicious internal attacks) as far as possible. Root access to critical servers and NAS systems should be completely blocked as far as possible or made as difficult as possible or secured.



Continuous Snapshots ensure in the Silent Brick System that all changes - including unwanted deletions - can be undone.

FAST LTA
We secure Petabytes.

2. Automatic inaccessible snapshots

At regular intervals, the backup storage should independently create snapshots that can only be deleted after the set retention period has expired. Changing the retention period must not be possible via standard accounts and should be secured by multi-factor authentication. The frequency and duration must be set to enable the highest possible security with just acceptable utilization. Since attackers often “look around” in the IT system for several weeks, the retention period should be chosen as long as possible.

3. Geo-redundancy

To protect against failure of entire instances or sites, backups should be replicated to a second site, if possible using functions anchored directly in the storage system that are not located in the normally accessible network (see above). The data storage at the second location must not be accessible from the main network, except for the purpose of replication.

4. Testing, Testing, Testing

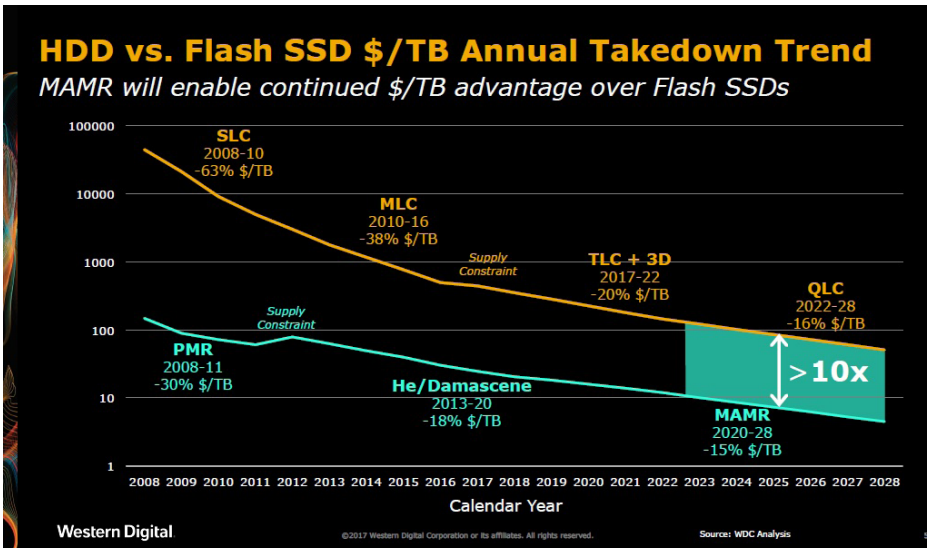
Both the verification of backups under quarantine conditions, as they prevail after an attack has occurred, and the recovery must be regularly checked and documented. It is also important to identify “single points of failure” that would make recovery completely impossible in the event of a failure, e.g., switches, routers, etc. Failure scenarios must be simulated for such components and the configurations adapted accordingly.

Since it is necessary for the optimization of the RTO (fastest possible recovery) that the data backup takes place where the data also occurs or is needed again, this central backup area should be implemented “on premises”, i.e. on site.

Can’ t this be done with flash storage...?

Flash storage is fast, but also expensive - (still) significantly more expensive than hard disk storage. Flash is now the standard for primary storage. For individual instances with limited capacity, the speed advantage outweighs the higher costs.

The situation is different when the security measures described above are implemented. If these are also implemented on the primary target – the flash storage – the cost difference is multiplied compared to hard disk storage. The longer storage time and the capacity required as a result do the rest to drive the costs into areas that are disproportionate to the achievable speed advantage. Instead of purchasing completely separate flash storage systems for the primary target area and thus increasing the complexity of the storage again, parts of the primary storage that may be available anyway can be allocated. If the secondary storage can be flexibly equipped with disk and flash storage, this can also be done directly in the backup storage if designed accordingly. It is obvious that due to the higher costs of flash storage, this area will be chosen as small as possible. A precise analysis of the RTO strategy is required in order to size the flash storage accordingly. Unlike disk backup, there are usually no special measures to protect against manipulation or deletion (snapshots). However, protection against the failure of individual data carriers through redundancy and the possibility of problem-free capacity expansion should not be dispensed with.



Many price forecasts ignore the fact that hard drive technologies are also constantly evolving. The manufacturer Western Digital is certain that flash storage will still be around 10x more expensive than hard drives in the future.

Conclusion:

Invest in secure disk backup

Flash storage is indispensable as the first storage instance and serves to fulfill the RTO objective. Air Gap and online archives can act as a “last line of defense” to protect against extreme emergencies, but are usually poorly accessible and thus delay the recovery of lost data.

Hard disk storage represents the best compromise between storage cost, performance and security. The more secure and comprehensive the central backup-to-disk area is, the smaller flash and air gap or online storage can be. This saves costs and manual effort without negatively affecting RTO and RPO. Since attacks are increasingly targeting the backup infrastructure first, disk backups must be specially protected not only against disk failures, but also against these attacks, for example through zero-trust, continuous snapshots and geo-redundancy.

The Silent Brick System is the complete storage solution for data protection - including flash memory, Air Gap and S3-compatible object storage. However, the focus here is also on backup-to-disk, which effectively protects against data loss and manipulation with multiple redundancy, continuous snapshots and replication.

PROULDY MADE IN EUROPE

FAST LTA
We secure Petabytes.

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