



CLOUD ARCHIVING

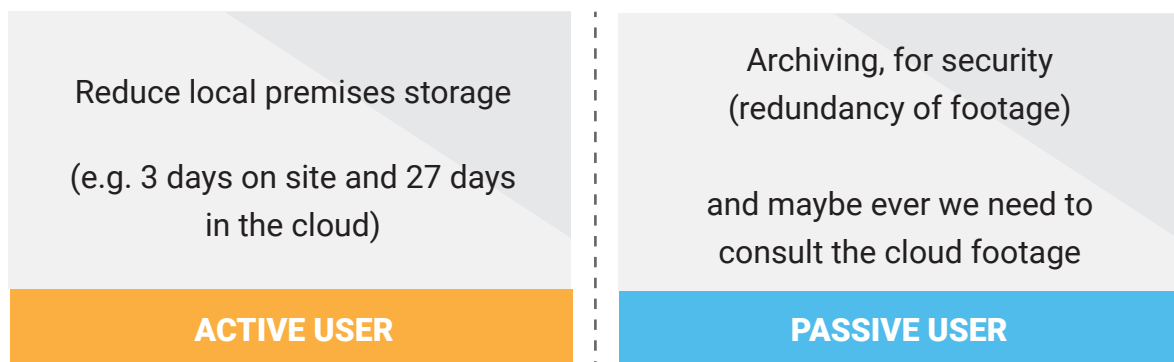
CA 05.18



Digifort : Cloud Archiving

Digifort can archive video evidence and backup files in the cloud for secure, off-site protection. This enables your video surveillance system and critical events can reduce the local on-site storage and use an independent different retention schedule for the cloud archive. This archiving process can be even custom scheduled in upcoming 7.3 version. Also the upcoming release incorporates now a, instant cloud playback optimization due to latency and bandwidth slowness's that can occur when remotely connect to the cloud storage.

As we see in our projects there are 2 main groups of users;



Active user are most common and the descriptions below are more directed to the active user.

When for example record for 3 days on-premises and 30 days of archiving retention in the cloud, there will an instant playback possibility which is native within the Surveillance Client. This will deliver a fast and seamless consulting of cloud archived footage without the need of complicated actions. Please note that in this case you will have 3 days of double footage, 3 days on premises and 3 days in the cloud + 27 days extra in the cloud. Those 3 days are mirrored so highly safe and secured for less risk on evidence loss.

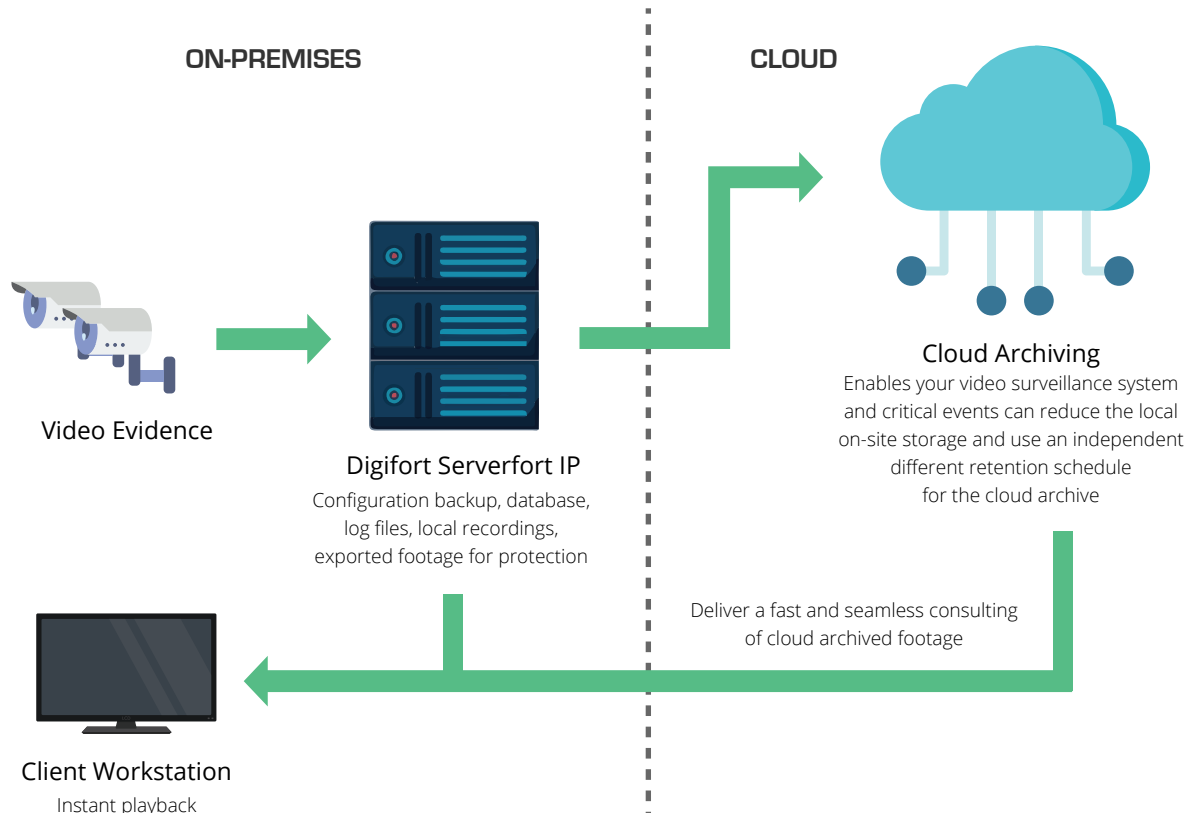
All Digifort system path's can be redirected to the same share on the Digifort server for the cloud storage, resulting in a cloud based backup of the system, including configuration backup, dbase, log files, local recordings, exported footage for protection... Disaster recovery can be deployed very easy and fast in the Digifort architecture.



Due to possible side effects linked to the cloud storage it must be calculated and designed correctly for enjoying the performance you need. The link between the Digifort Serverfort IP system on-premises and the cloud storage itself is internet, Digifort Cloud Archiving function needs to be able to push the footage and files fast enough to the client meaning the upload speed needs to be high enough. For rapid video evidence lookup the download speed from the cloud storage will become the main factor and also needs to be performant enough.

Digifort also recommend to be able to make sure the footage to the archive of 1 day can be pushed to the cloud within 1 day, otherwise the system will get behind with less secured evidence in the cloud.

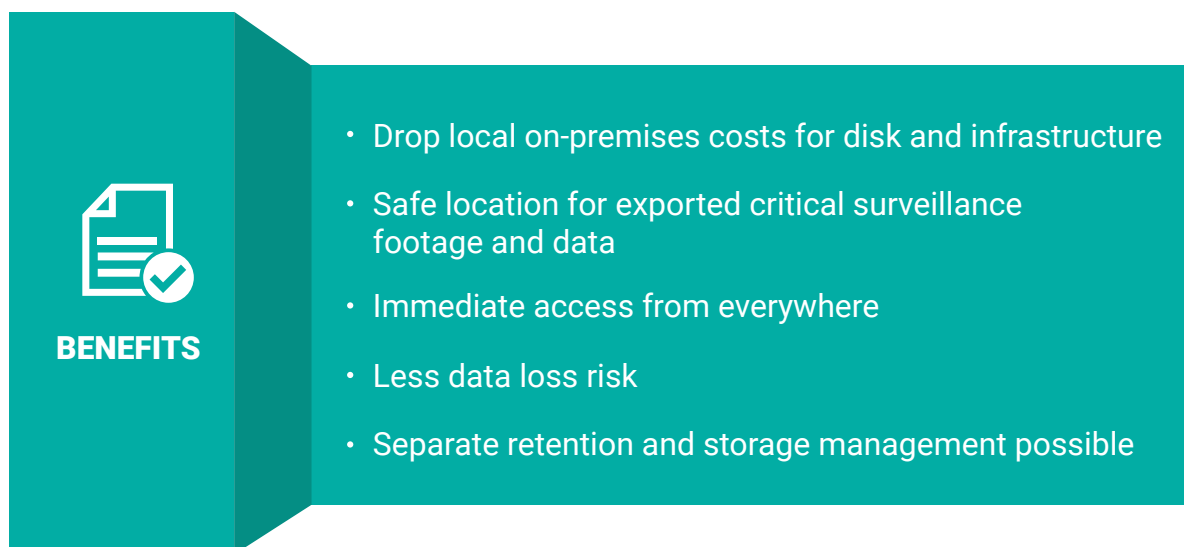
Simple file download to a non-site-connected Digifort Surveillance client workstation is also supported. When downloading for example 1 day of video evidence of 1 camera, the local player can playback for you this footage. Also this player can be used for passive users to review the downloaded footage first on their HDD from the cloud.



The way of connecting the cloud storage folder to the Digifort server must be configured as a logical drive in Windows. This results in a file based cloud storage program which are very performant. UNC network mapping can be used, or iSCSI, but we prefer SMB3.0 (native network unit) due to stability and performance. As for the cloud storage program itself all Digifort requires is File Storage, these are also the most economic packs by the vendors. Blob storage is not recommended for active users and not supported by Digifort due to no demand. Using middle ware to backup/sync to blob storage might be a solution.

The price calculation needs to be according to the amount of data the effective native recording folder shows. For example, if the total of your footage you would like to archive for 1 day is 10GB and you want to archive 30 days, you will need minimum 300GB of cloud storage. So based on this example it also will tell you the minimum upload time you need to have in order to transfer this 30GB/day to the cloud storage.

NOTE: the best tests have been made for active users was using Azure Storage General Purpose 2, also is very simple to map the drive to your server. Amazon S3 does not offers a native mapping service as far as we are informed and tested, therefore we do not recommend because a 3rd party plugin is required which generates an unnecessary extra point of failure. Glacier is also not recommended because is designed for archiving meaning the data is not meant to be accessed immediately and can take up to 4~5 hours before files are available while customers expect a more faster archive playback. This might be usable for passive users though.



BENEFITS

- Drop local on-premises costs for disk and infrastructure
- Safe location for exported critical surveillance footage and data
- Immediate access from everywhere
- Less data loss risk
- Separate retention and storage management possible



BENEFITS

- Fully automated
- Native Cloud playback with same Digifort client application
- Multi-site can be stored on same cloud storage (pooling)
- Downloaded edge recordings will also be pushed to the cloud
- Extendable in size at any time to follow your needs
- Protected for theft of local on-premises storage disks
- Plan yourself the archive schedule according to your resources
- Extremely high uptime of the storage
- All your data is mirrored in multiple datacenters depending to your vendor

! SUGGESTION

- Secure Data transit between Digifort and Cloud storage by using Client-Side Encryption by SMB3.0
- Use Cloud Disk Encryption
- Verify your internet upload speed to the cloud storage
- Verify your cloud storage download performance, the faster this is, the smoother cloud archive playback will work
- Due to archiving is a kind of folder copy, the available upload bandwidth will be used and is not controllable within Digifort
- For passive users, backup to blob cloud storage might be a solution (middleware). Digifort will archive in a folder that will be back upped in a blob cloud program
- Passive users might use a cheaper cloud storage program where first the footage needs to be downloaded to a local folder for then use manual playback (pay attention might take a very long time !)