White Paper | October 2022

Video storage in your Ava Cloud Video Security solution

Summary

Digital video surveillance systems, with their 24/7 usage, and near continuous need to save video data securely, place greater demands on the performance and reliability of the storage systems and drives than almost any other type of data storage workload.

Ava Security uses a combination of technologies that provide redundancy, resilience, and the ability to extend your data retention beyond that available from your cameras. These technologies provide secure storage both local to your cameras and network, and also using the cloud for a second tier of storage. Video stored either locally or to the cloud can be viewed from within the Ava Aware user interface.

This white paper outlines the approaches that Ava Security takes to provide the flexible storage for your important video data.

Storing video

The Ava Cloud Video Security solution enables you to use Ava Cloud Cameras, Ava Cameras without on-board storage, and third-party cameras in a single, cohesive system.

Where the video data is stored depends on the camera type:

- For Ava Cloud Cameras, the video is stored within the camera itself.
- For Ava Cameras without on-board storage, and for third-party cameras, the video is stored to the hard disk drives within the Ava Cloud Connectors.

You can configure your Aware video management system to save selected video data to the cloud, providing you with a second tier of storage to extend the retention periods of your cameras and to provide redundancy in the event of, for example, cameras being damaged or stolen, or your Cloud Connectors suffering an on-site network outage.

Ava Cloud Camera storage

All Ava Cloud Cameras include surveillance-grade microSD cards for the storage of your video data.

These memory devices are designed specifically to meet the demanding requirements placed in them by security cameras, such as the need for near-continuous recording, and being able to withstand changing environmental conditions.

Ava Cloud Cameras are fitted with microSD cards with appropriate storage for the cameras' specified data retention period.

Ava Cloud Connector storage

All Ava Cloud Connectors include multiple, high capacity surveillance-grade hard disk drives to ensure the best possible reliability of the drives to store your video data.

To prevent issues caused by failing drives, Ava Security uses a technique called *adaptive block-level erasure coding* to store data over multiple disks.

This technique is superior to traditional RAID solutions as it provides much greater flexibility and performance, giving fast and intelligent parity reconstruction, and dynamic block-level storage overhead.

(See "Appendix 1 — Ava Security's adaptive block-level erasure coding" on page 7 for detailed information.)

All video data stored on your hard disk drives is encrypted with the built-in encryption on the Ava Cloud Connectors.

Ava Cloud Storage

Ava Aware Cloud® provides the tools to enable you to automatically store your important video data to the Ava Cloud using Ava Cloud Storage™.

Ava Cloud Storage lets you securely copy the video data from your Ava Cloud Video Security solution and save that data to the Ava Cloud. It enables you to:

- Specify the type of data to be stored. You can choose to store a second tier copy of your Alarms, Anomalies, Saved Clips, all video defined as 'Interesting', and all video defined as 'Uninteresting'.
- Choose which of your Ava Cloud Cameras, Ava Cameras, and third-party cameras to have their data written to the Ava Cloud Storage.
- Define when your data is transferred to the cloud, so that your information is moved at the times when your network is at its quietest.
- Limit the bandwidth used by the uploads, so that transferring your important video data does not overwhelm your network.
- Choose the retention period. Your camera licenses include 30 days of storage for each licensed camera at no additional cost. You can purchase additional storage on a pay-as-you-go basis. Additional storage can be used to extend the data retention available from the local device.
- By default, your selected video data is written to the Ava Cloud. By using Ava Storage Connect™ you can store your data to your own cloud storage provider, or to save your video data to storage contained in your own local file system.

Data being sent to the cloud is routed directly between your Ava Cloud Camera and the Ava Cloud Storage.

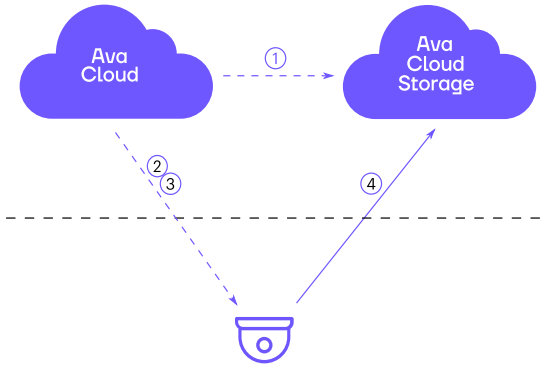

Figure 1 – Data sent directly from your Ava Cloud Cameras

Table 1 – Key to Figure 1

Step	Description
1	Aware configures the Cloud Storage and creates the access key with limited permissions
2	Aware creates the encryption key
3	Aware sends storage location, access key, and encryption key to Ava Cloud Camera
4	Encrypted data written to Cloud Storage

All data written to Ava Cloud Storage is encrypted with a key held within your own deployment. This key is not shared with Ava Cloud Storage.

In addition to storing the data from your Ava Cloud Cameras, you can also store the data from all your Ava Cameras without on-board storage and all your third-party cameras connected to your Ava Cloud Connectors. Again, in this case the encryption keys are stored within your own deployment and not within the Ava Cloud Storage.

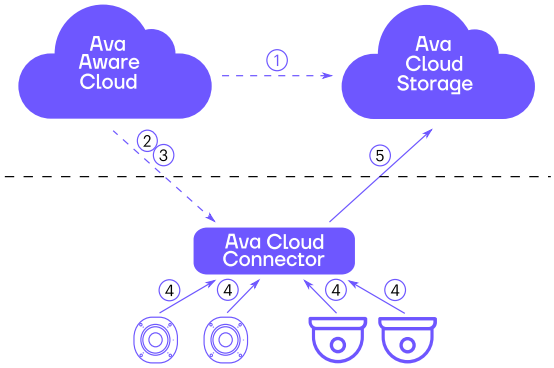

Figure 2 – Data sent from your Ava Cloud Connectors

Table 2 – Key to Figure 2

Step	Description
1	Aware configures the Cloud Storage and creates the access key with limited permissions
2	Aware creates the encryption key
3	Aware sends storage location, access key, and encryption key to Cloud Connector
4	Cameras stream video to Cloud Connector
5	Encrypted data written to Cloud Storage

Playback from device or storage

When viewing historic video that includes data saved in Ava Cloud Storage, Ava Aware first checks whether the required footage is stored locally on an Ava Cloud Camera or in an Ava Cloud Connector. Only if there is no local copy of the data, or the local device is not reachable is the video pulled from Ava Cloud Storage.

This enables you to view historical video from within the Aware user interface, regardless of where that video is stored.

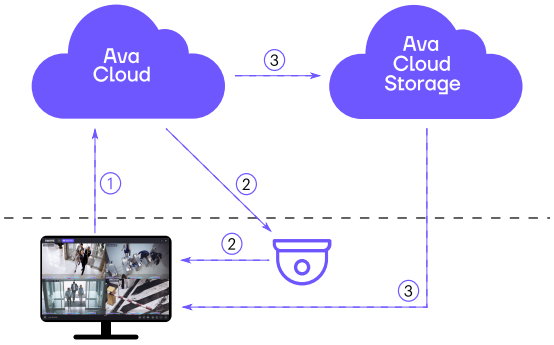

Figure 3 – Play historic video from device or Cloud Storage

Table 3 – Key to Figure 3

Step	Description
1	User requests historic video playback
2	Is device available with required data? If yes, play back from device
3	If device is not available, or does not have the data, check if cloud storage is available. If yes, encrypted data is retrieved from Ava Cloud Storage and viewed from Aware

Playing historic video directly from the Ava Cloud Camera or Cloud Connector whenever possible enables Aware to use Smart Path™ to optimize the data path, keeping the information within your own networks.

Configuring Cloud Storage

Cloud Storage is configured from within the Aware user interface. With just a few mouse-clicks, you select the data to be written to to Ava Cloud Storage, the retention period for the data, and set up your preferred upload schedule. You can choose multiple times and bandwidths to be used for your uploads, enabling you to configure the transfers to move the most data when your networks are at their quietest.

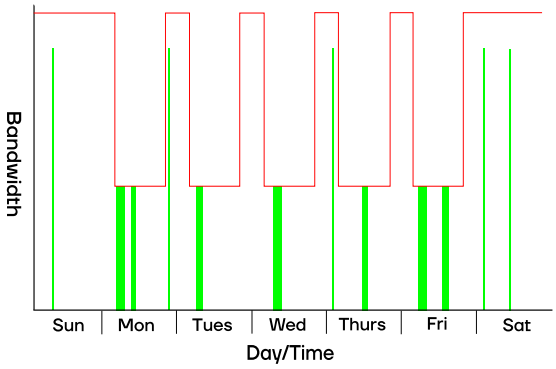

Figure 4 – Flexible data transfer schedules

Table 4 – Key to Figure 4

Line	Description
	Configured bandwidth limits (example)
	Consumed bandwidth (example)

Security of stored data

All data saved to Ava Cloud Storage is encrypted using the unique keys held by your own Ava Aware Cloud deployment, ensuring your data cannot be compromised. Only those users that have accounts created in Ava Aware Cloud, and that have suitable viewing permissions can access and decrypt the stored recordings. Your Aware administrators have the ability to create and disable user accounts, so, with Ava, you have full control over who can access your recordings.

Data pruning

For Ava Cloud Cameras, data is removed either when:

- The retention period you configured in Aware Cloud has expired.
- When there is no available storage remaining on the Ava Cloud Camera.

Data is removed from Ava Cloud Storage either when:

- The retention period you configured in Aware Cloud has expired.
- The licensed time period for your Ava Cloud Storage has been reached.

Your Ava Cloud Storage is not impacted in the case where data is pruned from the camera due to a lack of storage space. This means you can purchase and configure much longer durations of cloud storage for a camera than the camera can handle locally.

For example, a 30 day Ava Cloud Camera (such as a DOME-W-30) can be paired with 120 days of cloud storage. This allows 120 days of video to be kept in the cloud, as well as the most recent data to also be stored and available from the camera itself.

To archive and keep the Saved Clips — video that you have specifically bookmarked — you can save them to your extended Ava Cloud Storage, and you can also download them locally to keep a permanent copy of the footage.

Physical location of storage

Ava Cloud Storage is hosted in partner data centers that are certified to SOC 2, ISO 27001, and Payment Card Industry Data Security Standard (PCI-DSS).

Ava use data centers in Plano Texas and Toronto for customers based in North America, Sydney for Australian customers, and Amsterdam for customers within Europe.

Ava Storage Connect — local storage using CIFS

With the purchase of a suitable Ava Storage Connect license, you have the ability store your video data to your own local Common Internet File System (CIFS) compatible storage.

Using local storage

Once you have configured your backup CIFS locations from within Aware, your deployment decrypts the video from your selected cameras and creates video segments that are saved as .MP4 files on your local storage. You have the same options about what you choose to record as you do for the Ava Cloud Storage — you can choose to store Alarms, Anomalies, Saved clips, video that is Interesting, and video that is Uninteresting.

Your CIFS-compatabile storage must be routable from the Ava Cameras or Ava Cloud Connectors in order for your video to be stored on your local storage.

You can play back the video saved to your CIFS system from within Aware (providing you have connectivity between Ava Cloud and the CIFS server), and you can also view the video clips using any .MP4 player software by browsing to the .MP4 files.

Security of stored data

Your video clips are stored unencrypted on your own file system, so you must make suitable arrangements to ensure the security of the storage and to limit access to the stored video. Aware uses the encryption that is configured on the CIFS connection to protect the video being played back from local storage.

Conclusion

The redundancy and resilience of your video data is provided by the design of each component within your Ava Cloud Video Security solution.

All Ava Cloud Connectors include state-of-the-art hard disk drives specifically designed for use in digital surveillance systems.

Ava Cloud Cameras include on-board surveillance-grade storage. By using these specially selected storage devices, your data benefits from the best available local storage solutions.

From Aware Cloud, you can use Ava Cloud Storage to store a second tier of the video data that is most important to you. You can write this data to the Ava Cloud, or use Ava Storage Connect to copy it to your preferred cloud storage provider, or to storage within your own local file system. This provides redundancy and the ability for you to extend the the retention available to your Ava Cloud Cameras, as well as for your Ava Cameras and third-party cameras connected to Ava Aware Cloud via your Ava Cloud Connectors. You can view historic video from within the Ava Aware user interface, without having to decide whether you want to view footage stored on a device in your local network, or from your Ava Cloud Storage.

Appendix 1 — Ava Security's adaptive block-level erasure coding

Ava Security developed the patented adaptive block-level erasure coding method used on the Ava Cloud Connectors to ensure that important data is not lost in the event of a hard disk drive failing.

In a similar method to RAID 5 and RAID 6, erasure coding involves creating additional parity data that is stored alongside the original data. This parity data can then be used to recover the original data if it becomes lost.

The Ava Security storage system by default operates at the following parity levels:

- **2 disks**: Data mirrored
- **3-5 disks**: One parity block
- **>=6 disks**: Two parity blocks

Within the Ava Aware software, every piece of video data to be stored is split into multiple data fragments.

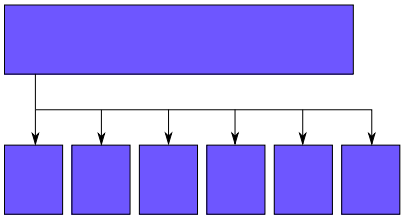

Figure 5 – Incoming video is split into fragments

From these fragments, additional parity fragments are calculated, and then stored across multiple drives.

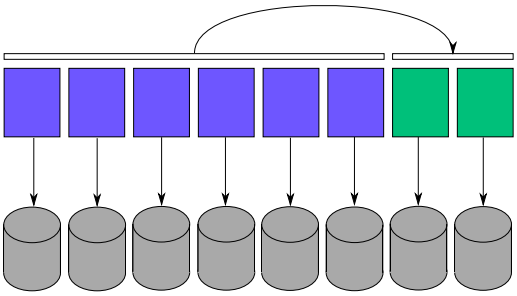

Figure 6 – Aware calculates the parity fragments

The total number of fragments corresponds to the number of available drives, which in this example is 8. The number of parity fragments corresponds to the number of drive failures that can be tolerated before the data becomes unrecoverable.

If one or more drives fails, the data from the failed drives can be rebuilt from the remaining fragments.

This is done by reading the available fragments from the remaining disks. The missing fragments are reconstructed using the parity fragments and the remaining data fragments, and then the original data is restored by combining all the data fragments.

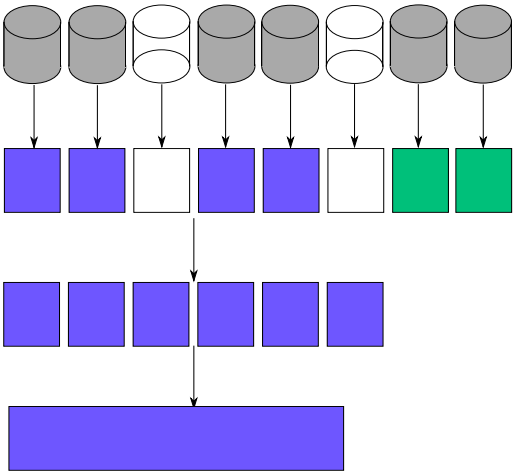

Figure 7 – Video data reconstructed after disk failures

Intelligent reconstruction of data

In traditional RAID arrays, there is no understanding of the data stored on them, and so on a disk failure, the entire array is rebuilt — a very slow and wasteful process.

Assuming 10MB/s of reserved performance for reconstruction, in a RAID 5/6 array, it requires 4.5 days to rebuild a 4TB disk. During this time the array operates in a degraded mode and is vulnerable to subsequent failures. If the system is operating on a 7 day retention period, most of that rebuild is wasted.

Alternatively, using RAID 10 gives easy rebuilds and good performance, but at the cost of wasting 50% of the available storage.

With Ava Security adaptive block-level erasure coding, all new data is immediately written to all available disks, ensuring it is at the correct resiliency level straight away. The old data is rebuilt on a newest-first basis, ensuring any unretained data is not wastefully rebuilt, so the overall array performance does not degrade.

Ava Security adaptive block-level erasure coding provides similar speeds to RAID 10, with the improved disk utilization of RAID 5/6, giving you the best features from each configuration.

Dynamic parity control

Aware carries out the erasure coding in software, and dynamically responds to disk failures by either preserving or changing the parity level.

When a single disk fails, the total number of fragments is reduced by one, and the system can either reduce the parity level, or start splitting the data into fewer data fragments to keep the same parity level.

For example, if there were 7 drives available, the data could continue to be split into 6 data fragments and 1 parity fragment:

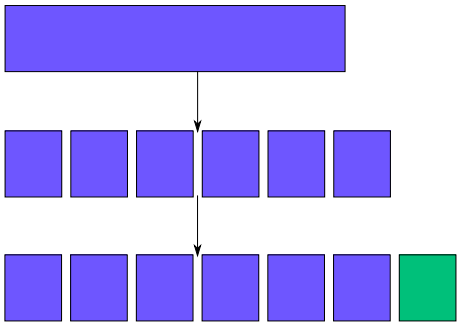

Figure 8 – Aware sets 6 data and 1 parity fragments

Alternatively, the data could instead be split into 5 data fragments and 2 parity fragments.

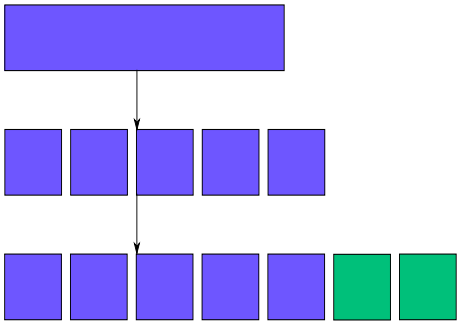

Figure 9 – Aware sets 5 data and 2 parity fragments

This means that data stored after a single failure can still be as resilient to further failures. This is not the case for RAID systems, which always reduce the resiliency levels when a drive fails.

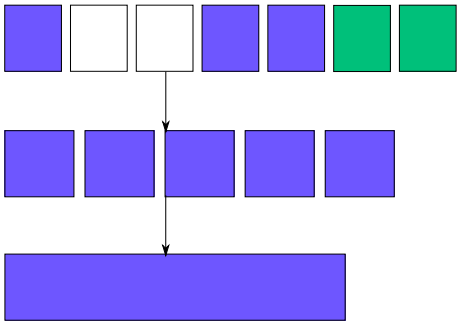

Figure 10 – Video data reconstructed after further disk failures

The Ava Security system can also dynamically vary the parity level as it stores data. It can do this based on a range of factors, allowing the system to record the most important data with additional resiliency, and less important data with lower resiliency.

For example less important data could be stored with 2 parity fragments, and more important data with 3 parity fragments.

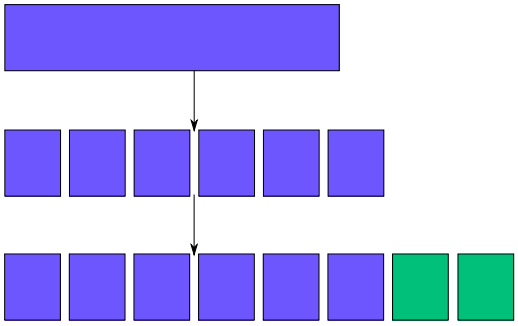

Figure 11 – Less important data saved with 2 parity fragments

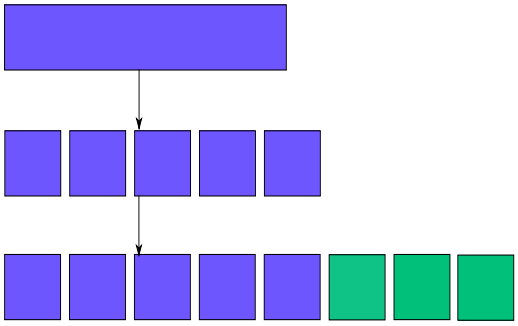

Figure 12 – More important data saved with 3 parity fragments

Security

A global company with offices in the UK, Norway, and the US, Ava delivers better, smarter security.

Organizations use the Ava Aware® open video security data platform to protect people and operations, allowing them to optimize for their evolving business needs, giving them more time to spend on the possibilities ahead.

To learn more about Ava's intelligent solutions and how you can enjoy proactive security, visit our website or schedule a demo with a member of our sales team at sales@avasecurity.com.

www.avasecurity.com

White paper first published March 2020, updated October 2022.