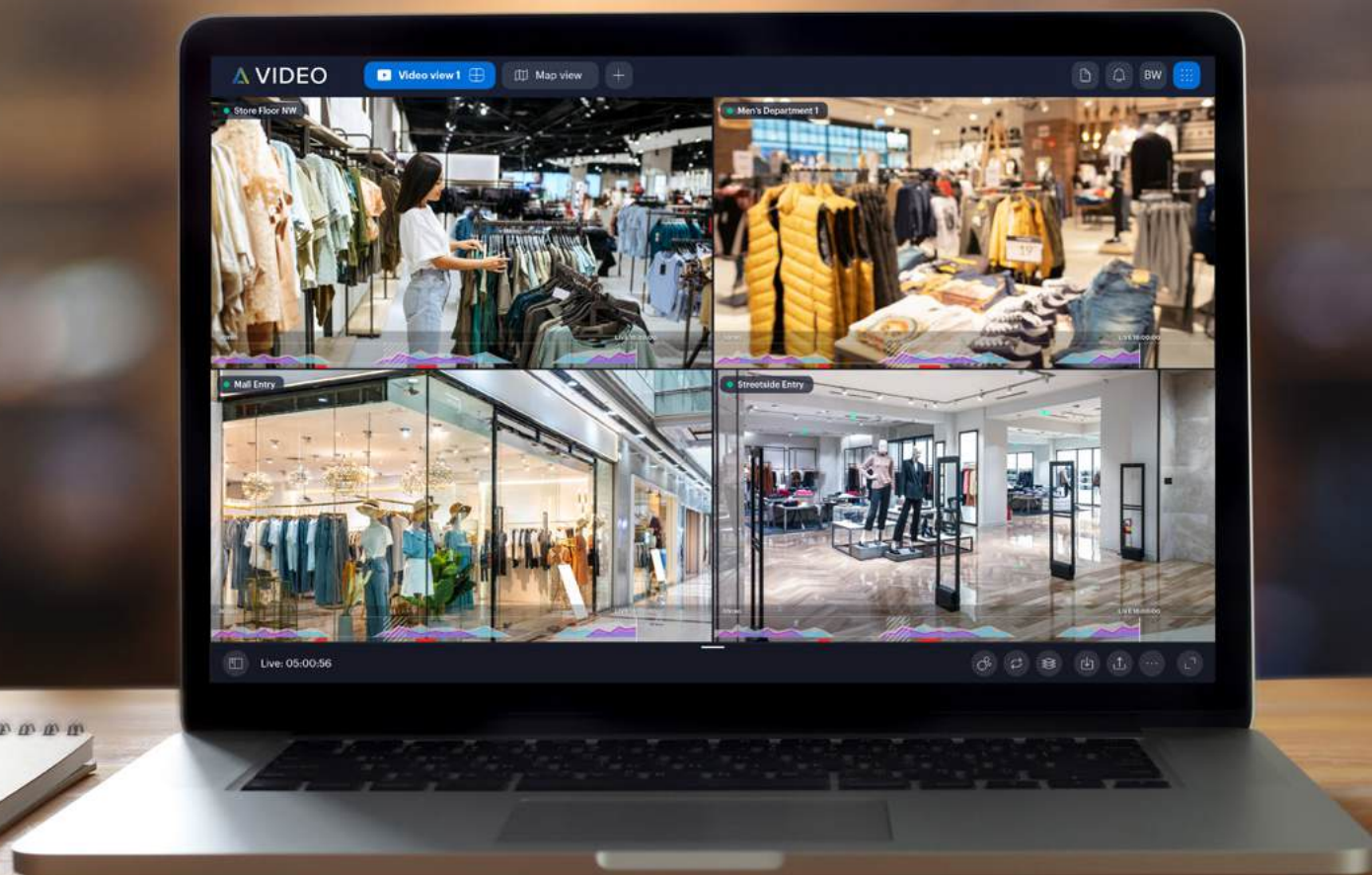




Video storage in Alta Video

With Avigilon Alta Video

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.

Avigilon Alta Video 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 Alta Video web app or the Alta Video mobile apps.

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



Storing Video

Avigilon Alta Video enables you to use Alta cloud-native cameras, Avigilon 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 Avigilon Alta cloud-native cameras, the video is stored within the camera itself.
- For Avigilon cameras without on-board storage, and for third-party cameras, the video is stored to the hard disk drives within the Alta Cloud Connectors.

You can also configure your Alta Video deployment to save selected video data to the Alta Storage 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.

Alta cloud-native camera storage

All Alta cloud-native 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.

Alta cloud-native cameras are fitted with microSD cards with appropriate storage for the cameras' specified data retention period.



Alta Cloud Connector storage

With multiple, high capacity surveillance-grade hard disk drives on all but the smallest capacity Alta Cloud Connectors, the Cloud Connectors are designed to provide the best possible reliability of your stored video data.

To prevent issues caused by failing drives, Alta Cloud Connectors use a patented technique—adaptive block-level erasure coding—to store your 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: Adaptive block-level erasure coding” for detailed information.

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

Alta Storage Cloud

Avigilon Alta Cloud provides the tools to enable you to automatically store your important video data to the Alta Cloud using the Alta Storage Cloud.

Alta Storage Cloud lets you securely copy the video data from your Alta Video deployment and save that data to the Alta 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 Alta cloud-native cameras, Avigilon cameras without on-board storage, and third-party cameras to have their data written to the Alta Storage Cloud.
- 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 Alta Storage Cloud. By purchasing Alta Storage Connect licenses, 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 Alta cloud-native camera and the Alta Storage Cloud.

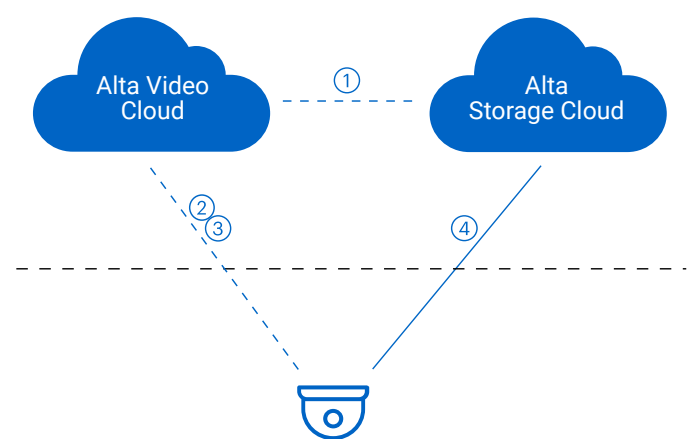


Fig 1: Data sent directly from Alta cloud-native cameras

TABLE 1 – KEY TO FIGURE 1	
STEP	DESCRIPTION
①	Alta Video configures Alta Storage Cloud and creates the access key with limited permissions.
②	Alta Video creates the encryption key
③	Alta Video sends the storage location, access and encryption keys to the Alta cloud-native camera
④	Encrypted data is written to Alta Storage Cloud



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

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

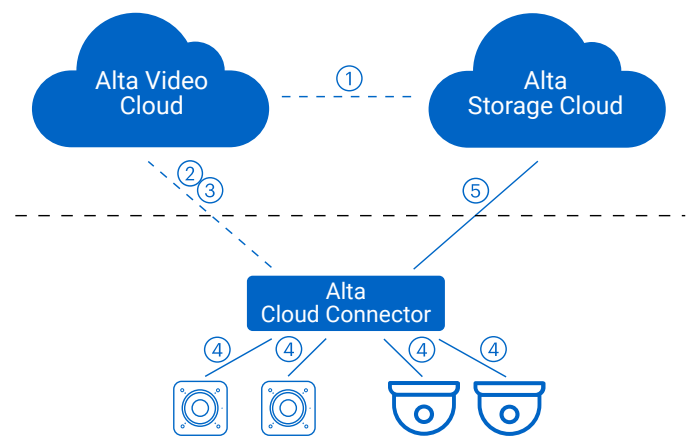


Fig 2: Data sent from your Alta Cloud Connectors

TABLE 2 – KEY TO FIGURE 2	
STEP	DESCRIPTION
①	Alta Video configures Alta Storage Cloud and creates the access key with limited permissions.
②	Alta Video creates the encryption key
③	Alta Video sends the storage location, and the access and encryption keys to the Alta Cloud Connector
④	Cameras stream video to Alta Cloud Connector
⑤	Encrypted data is written to Alta Storage Cloud

Playback from device or storage

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

This enables you to view historical video from within the Alta Video web app or Alta Video mobile apps, regardless of where that video is stored.

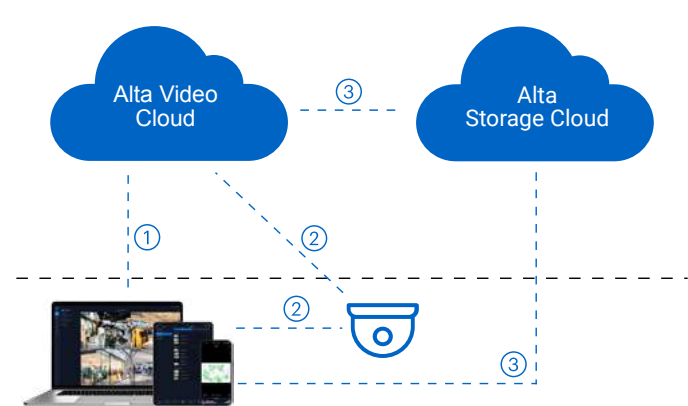


Fig 3: Play historic video from device or Alta Storage Cloud

TABLE 3 – KEY TO FIGURE 3	
STEP	DESCRIPTION
①	User requests historic video playback
②	Is the device available with required data? If yes, play back from device.
③	If the device is not available, or does not have the data, check if cloud storage is available. If yes, encrypted data is retrieved from Alta Storage Cloud and viewed from Alta Video web app or Alta Video mobile apps.

Playing historic video directly from the Alta cloud-native camera or Alta Cloud Connector whenever possible enables Alta Video to use Smart Path™ to optimize the data path, keeping the information within your own networks.



Configuring Alta Storage Cloud

Alta Storage Cloud is configured from within the Alta Video web app. With just a few mouse-clicks, you select the data to be written to Alta Storage Cloud, 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.

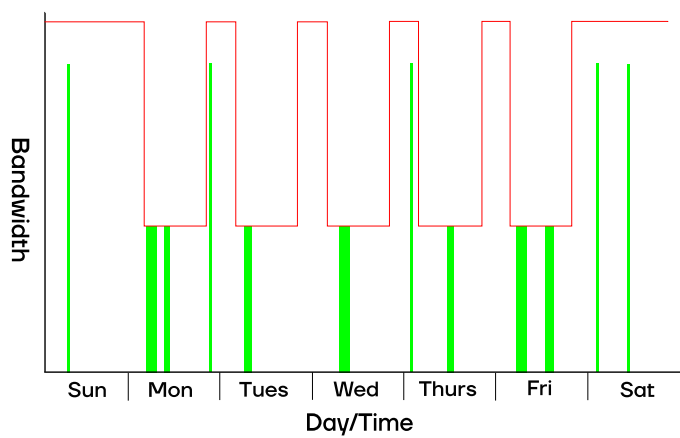


Fig 4: Flexible data transfer schedules

TABLE 4 – KEY TO FIGURE 4	
STEP	DESCRIPTION
—	Configured bandwidth limits (example)
—	Consumed bandwidth (example)

Security of stored data

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

Data pruning

For Alta cloud-native cameras, data is removed either when:

- The retention period you configured in Alta Storage Cloud has expired.
- When there is no available storage remaining on the Alta cloud-native camera.

Data is removed from Alta Storage Cloud either when:

- The retention period you configured in Alta Video has expired.
- The licensed retention period for your Alta Storage Cloud has been reached.

Your Alta Storage Cloud 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 Alta cloud-native camera (such as a DOME-W-30) can be matched 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 Saved Clips — video that you have specifically bookmarked — you can save them to your extended Alta Storage Cloud, and you can also download them locally to keep a permanent copy of the footage.

Physical location of storage

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

For European customers, the video storage is hosted in Amsterdam. For US customers the video storage is hosted in Plano, Texas.



Conclusion

The redundancy and resilience of your video data is provided by the design of each component within your Alta Video deployment.

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

Alta cloud-native 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 Alta Video, you can use Alta Storage Cloud to store a second tier of the video data that is most important to you. You can write this data to the Alta Storage Cloud, or use Alta 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 retention available to your Alta cloud-native cameras, as well as for your Avigilon cameras without on-board storage and third-party cameras connected to Alta Video via your Alta Cloud Connectors. You can view historic video from within the Alta Video web app, or the Alta Video mobile apps, without having to decide whether you want to view footage stored on a device in your local network, or from your Alta Storage Cloud.

To learn more, visit: www.avigilon.com



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2026 Motorola Solutions, Inc. All rights reserved. 01-2026 [JMS03]

Appendix: Adaptive block-level erasure coding

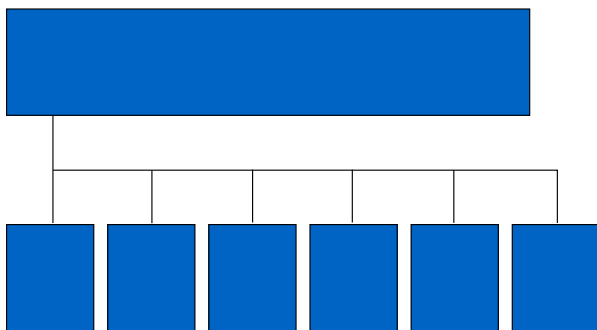
Avigilon Alta developed the patented adaptive block-level erasure coding method used on the Alta Cloud Connectors to ensure that important data is not lost in the event of a hard disk drive failing.

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 Avigilon Alta storage system by default operates at the following parity levels:

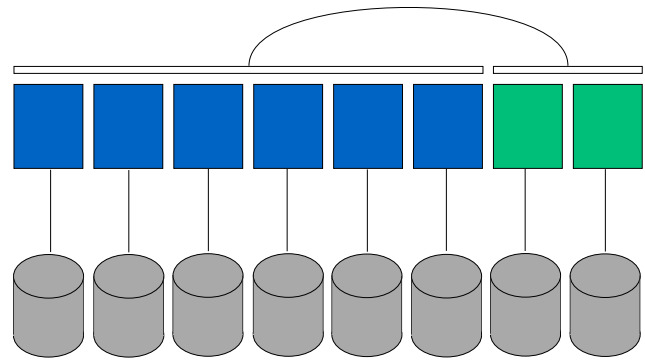
- 1 disk: No parity
- 2 disks: Data mirrored
- 3-5 disks: One parity block
- ≥ 6 disks: Two parity blocks

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



Incoming video is split into fragments

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

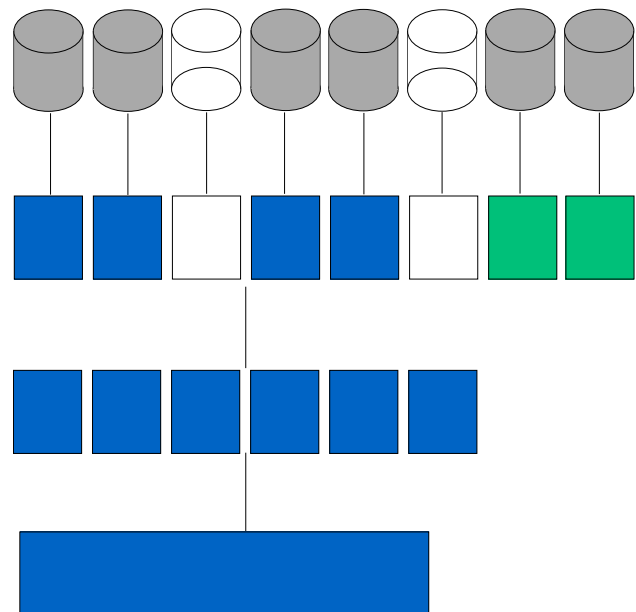


Alta Video calculates the parity fragments

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.



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 Avigilon Alta 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.

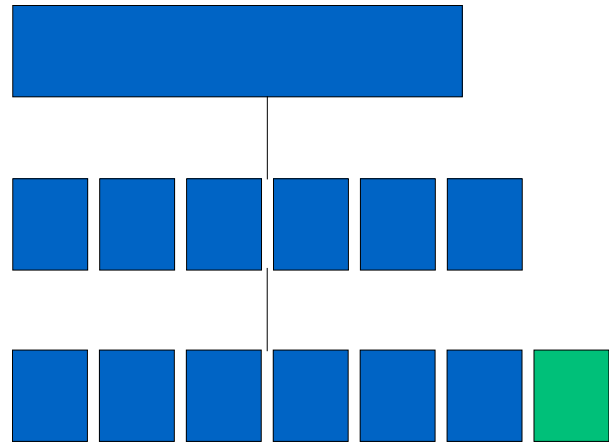
Avigilon Alta adaptive block-level erasure coding provides similar speeds to RAID 10, with the improved disk utilization of RAID 5/6, giving you the best features from each configuration.

Dynamic parity control

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

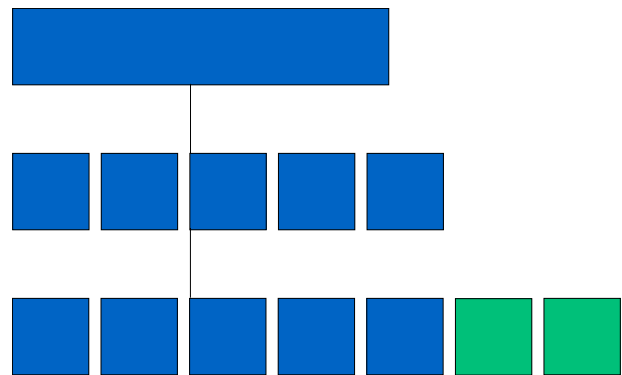
When a single disk fails, the total number of fragments is reduced by one, and the system can either reduce the parity level, or start splitting the data into fewer data fragments to keep the same parity level.

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



Alta Video sets 6 data and 1 parity fragments

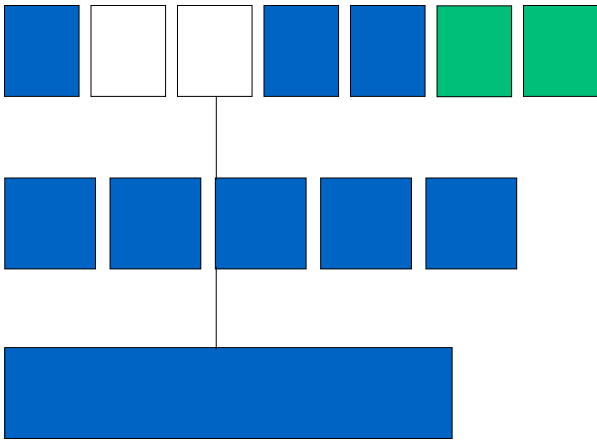
Alternatively, the data could instead be split into 5 data fragments and 2 parity fragments:



Alta Video 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.

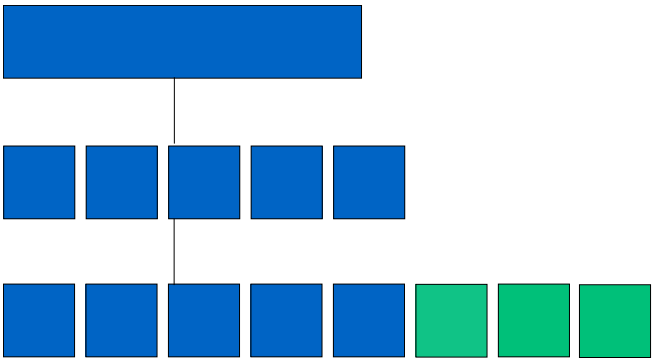




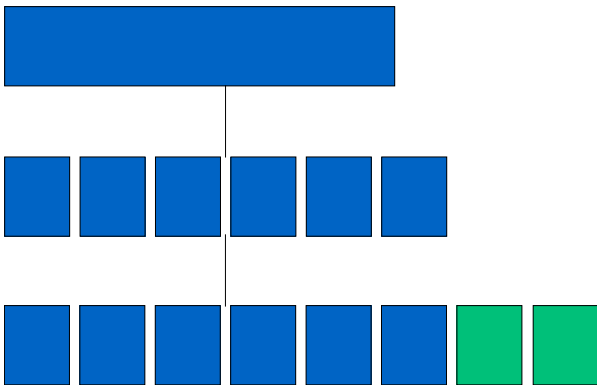
Video data reconstructed after further disk failures

Alta Video 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.



More important data saved with 3 parity fragments



Less important data saved with 2 parity fragments

