

Surveillance data storage: What you need to know



Video surveillance is becoming smarter and more effective than ever as a way to fight crime, discover the causes of accidents for better prevention and to help find missing people. All those cameras mean a lot of video data being sent to storage devices.

These Surveillance Digital Video Recorders (sDVR) and Surveillance Network Video Recorders (sNVR) need to be built to withstand that huge barrage of data coming at them from multiple sources and often at high bandwidths. When it comes to longer term server storage, data needs to be retained for years without dropping frames, while still being accessible to video management systems and all while providing fast access to imagery for analysis.

Maintaining these storage solutions under the huge data pressures, which are only going to get greater, requires a very specific solution. The result are drives which are made specifically for the needs of surveillance. But what are these needs and how do they work?

What causes drive data to be lost or damaged?

The warranty of a drive typically gives you a number of years before that drive should to be replaced in order to maintain safe operation. But the warranty only offers those years of secure and reliable life based on a number of external factors being within a certain range. This is why it is important to understand those factors and control them in order to get the most accurate measure of reliability for long term security. So, what are these factors?

One of the major considerations that can affect how long a drive lasts is the operating temperature. At the centre of a drive is a fluid dynamic bearing that is responsible for the platters, which store the data, spinning correctly. Since this bearing uses oil as a lubricating fluid, any prolonged increase in temperature can cause that fluid to become thinner and ultimately leak. In the long term a leak of this kind will increase the chance of failure.

This is a way that surveillance grade drives offer an improvement even over enterprise grade drives. This is because surveillance drives can typically operate within a temperature range of 0 to 70 degrees Celsius whereas an enterprise drive would only be rated 5 to 55 degrees Celsius. In order to maintain enterprise drives at a large scale, one would need to spend more on actively cooling the room. While the enterprise drive may seem to have a more appealing warranty or rated workload, this may require additional environmental controls when used in a demanding, heat causing, surveillance scenario, which would end up costing more.

The rated workload is another area to look out for. This refers to wear which a spinning drive will inevitably suffer with all that movement. The amount of work that drive does, in terms of reading and writing data, will affect the amount of wear and the rated workload. For surveillance drives the typical rating is up to 180 TB/year. Although this is low compared to enterprise drives, at 550 TB/year, it is considerably higher than the 55 TB/year defined for client use drives.

How can drive storage stability be predicted and planned?

Surveillance storage is typically a 24/7 system that requires constant work from the drives storing the video data. The requirement of the drive to keep working is called the operating duty. While a home desktop computer or laptop might feature hard drives built for hours of daily use, “always-on” surveillance is far more demanding. Since surveillance drives are never powered down, they need to work very differently to client drives.

Of course, even the best drive will still reach the point where a failure eventually occurs. But this can be factored in too by using the Mean Time to Failure (MTTF) measure. This is a statistical measure of how long it takes on average until a drive failure would be expected. A typical MTTF is 1 million operating hours, which translates into 114 years. But it needs to be understood that it’s listed not for a single drive but for a larger statistical population of HDDs. So, in a cluster of one million drives you could expect one to fail every hour. To put that in more realistic terms, for a 500-drive cluster, an error can be expected every 2,000 hours or at around 83 days.

Taking this further you can calculate the Annualized Failure Rate (AFR) using the MTTF data. This would reveal that a one-million-hour-MTTF drive setup with 500 drives could expect five drives to fail each year. This data can then be used so that the operator can budget for drive replacements to ensure the safest storage of data.

Which is the best drive for surveillance?

The most pertinent factor when buying drives for many users may initially be capital expenditure. However, it's important to look at the longer-term operational expenditure before hurrying to save money at the start with cheaper drives that, ultimately, could result in higher costs in the longer-term through maintenance and servicing expense.

Enterprise drives lack the hardware and software enhancements to support the video write workload while drives designed for client use are not suited to 24/7 operation.

Surveillance specific drives, such as Toshiba’s S300 Surveillance or V300 Video Streaming HDDs, promise to fulfil their defined specifications that can be relied on including a one-million-hours MTTF rating over a three-year warranty, as well as an operational temperature range of 0 to 70 degrees Celsius. They also offer a buffer up to 256MB and optimised disk controllers allowing up to 64 HD video feeds to be written at once. Dynamic Cache Technology also helps to improve the real time performance of the drives so that no frames are dropped, even under high strain workload situations such as writing and reviewing videos at the same time.