Quantum®

COST-EFFECTIVE VIDEO STORAGE

IN COLLABORATION WITH

PoliceOne

Introduction

Law enforcement agencies continue to expand their use of body-worn cameras (BWCs) to meet public demand for greater accountability and transparency in police operations. While body-worn cameras may address those problems, they also give rise to another: How can agencies manage the mammoth volume of video files they produce? Server capacity that is way past what most local police agencies have on hand is critical, and storage of that video on someone else's server is expensive.

Body-worn camera video is just the latest addition to the volume of digital evidence used in police operations and investigations. Law enforcement agencies were already coping with video from vehicle-mounted recorders and interview rooms, still camera images and audio recordings of wiretaps and interviews. Gigabytes (GB) of files quickly grow to become terabytes (TB) and petabytes (PB), and the growing volume of data exceeds the capacities of most in-house data stores.

The problem is aggravated by the lack of dedicated IT staff in most police agencies. There are over 18,000 law enforcement agencies in the United States, and 73 percent of these have fewer than 25 sworn personnel. Small operations like this do not have an IT staff to help them manage large data volumes. They are dependent on the people they have on staff, most of whom have minimal technical expertise.

[i] Census of State and Local law Enforcement Agencies, 2008. http://www.bjs.gov/content/pub/pdf/csllea08.pdf

[ii] Vern Sallee, "Outsourcing the Evidence Room: Moving Digital Evidence to the Cloud," The Police Chief 81 (April 2014): 42–46.

[iii] https://www.policeone.com/police-products/body-cameras/articles/8243271-For-police-body-cameras-big-costs-loom-in-storage/

[iv] http://www.nj.com/news/index.ssf/2015/11/nj_motor_vehicle_commission_computers_down_1.html

[v] https://iq.quantum.com/exLink.asp?255175440V63K67I101187216&CS00309A

The Unseen Cost of Video Storage

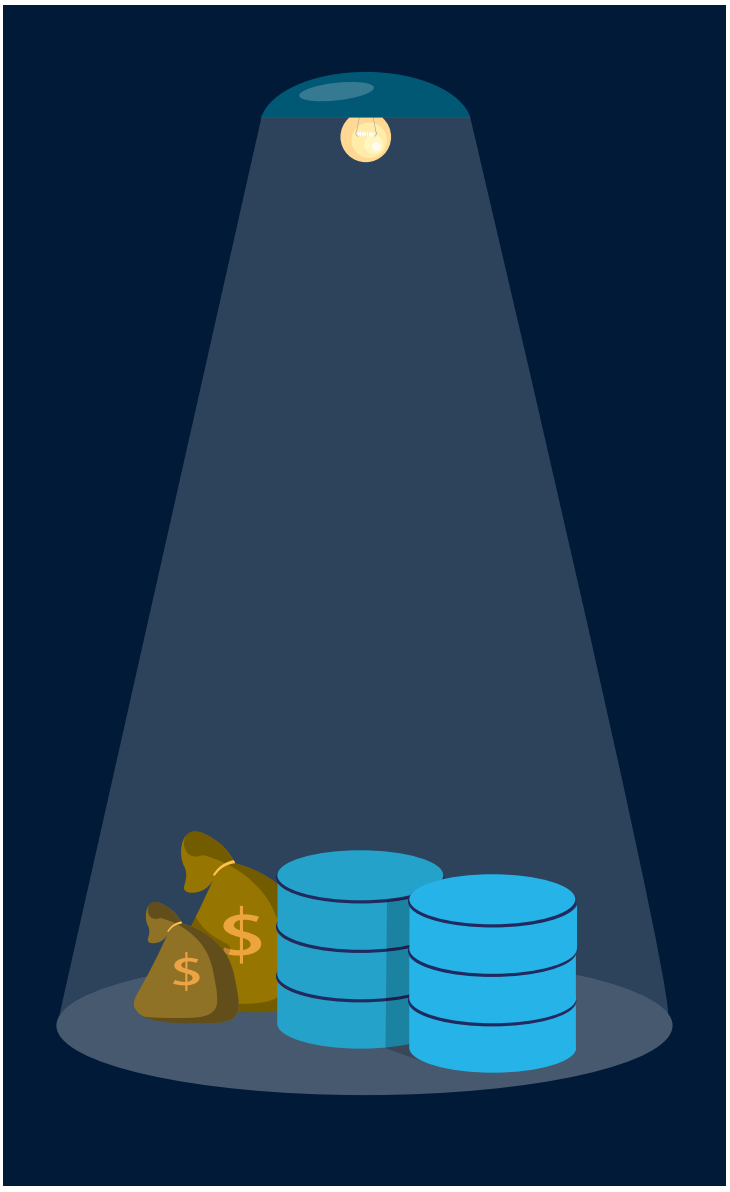
When adopting a body camera program, many may view the upfront price as the majority implementation cost. Body-worn cameras designed for the hazards law enforcement officers encounter each day typically cost $700-$1,500 each, depending on manufacturer and features. The cost of video data storage is less evident.

Most BWC vendors offer some type of data management solution with their hardware, consisting of a "front end" indexing and retrieval software package, plus an allotment of online storage space for the video. These data management plans are usually priced on a per-camera or per-user basis, providing a few GB of storage space. With half an hour of video coming in at around 800MB and officers producing four hours of video per day—a single officer might generate a terabyte of video per year. This far exceeds the allocation most vendors will provide without a surcharge.

It's possible to purchase a contract to store all the video an agency produces, but it comes with a high price tag. One such plan offers unlimited storage for $1,000 per year per officer. An agency with 1,500 sworn officers would spend $3 million in storage costs alone over two years.

Data storage costs can derail a BWC program:

- The Baltimore Police Department, suffering from a dearth of public trust and multiple episodes of police brutality claims, saw a BWC program as a positive step in rebuilding its image. Even so, when the mayor saw that video storage alone would cost the city $2.6 million per year, she vetoed the program.
- San Diego Police paid $267,000 for 1,000 cameras, plus another $3.6 million for storage, maintenance contracts and other program expenses.
- The Duluth, Minnesota PD spent just $5,000 for cameras, but $78,000 for data storage.
- The Los Angeles Police Department's BWC program was postponed when City Hall saw the price tag: $57.6 million over five years.



How retention policy affects storage costs

A major factor of storage costs is the agency's retention policy. How long does the department have to keep the video available before it can be deleted so that space is freed up for other files? "Forever" might be a desirable policy, but that would mean multiplying storage costs every year as the archive grows. Some states mandate the time law enforcement agencies have to maintain records, but most leave it up to the individual department to determine its own policy.

Retention policies are based on the predicted need to access the files. Video files documenting traffic stops or field interviews, where no enforcement action is taken, might be retained for 30 days if there is no complaint or other complication that involves them. Recordings of misdemeanor arrests could be kept for two years, or until the case is fully disposed of, with felony cases retained longer.

A video with evidence in a major felony case or one that was subject to civil litigation might be retained indefinitely. As each case ages, the need to have the video available for immediate review typically decreases, and a delay of a few minutes before the file can be available is acceptable.

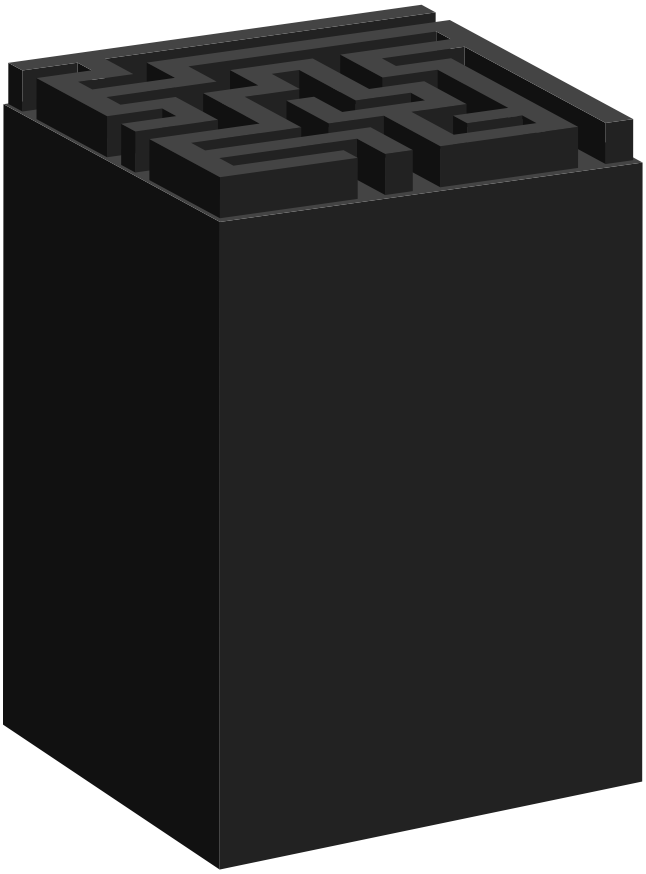
Active management of such a system is an ongoing, dynamic process. New files are added constantly, and aged files that can be purged under the retention policy need to be removed to make room. This means one or more full-time staff members is needed for IT duties that keep the storage volume from being overwhelmed. Poor storage management gives rise to the day there is no room on the server to upload video from that day's patrols, or the deletion of a file critical to a major case.

Storage: What are the options?

Option 1: On-premise storage

The simplest and most obvious storage solution is for agencies to maintain their video archives on-site, as most do with paper reports and other hard-copy records. In practice, this doesn't work for most police forces.

For a few thousand dollars, an agency can purchase a network attached storage (NAS) box, stuffed with multiple spinning hard disks in a RAID (Redundant Array of Independent Disks) array that appear as a single drive to a connected computer. Depending on how the RAID array is configured, this can even provide for on-site backup to guard against the problem of a deleted or corrupted file. In practice, this solution quickly becomes problematic:



- An agency of only 10 officers might generate 10TB of data per year from BWCs alone, exceeding the capacity of many storage systems.
- Other video from interview rooms, patrol car cameras, security camera ouput, and other miscellaneous digital evidence aggravates the storage and management problem.
- Without some tricky work-arounds, Windows (the most common operating system used in business) will not recognize drive volumes larger than 2TB. This means having to index and track files on multiple drive letters.
- The complexity of security settings leaves the agency open to having files deleted or edited without authorization.
- The NAS box provides a single point of failure. If that device is damaged or stolen, it takes the entire archive with it. An off-site backup is a crucial need.

Option 2: Cloud storage

Online or "cloud" storage is the most common storage medium, as few agencies want to invest the money, time and training to construct their own on-site storage networks. The solution offered by most BWC vendors is 100 percent online, with the vendors reselling storage space purchased from a major data store like Amazon Web Services (AWS) or Microsoft.

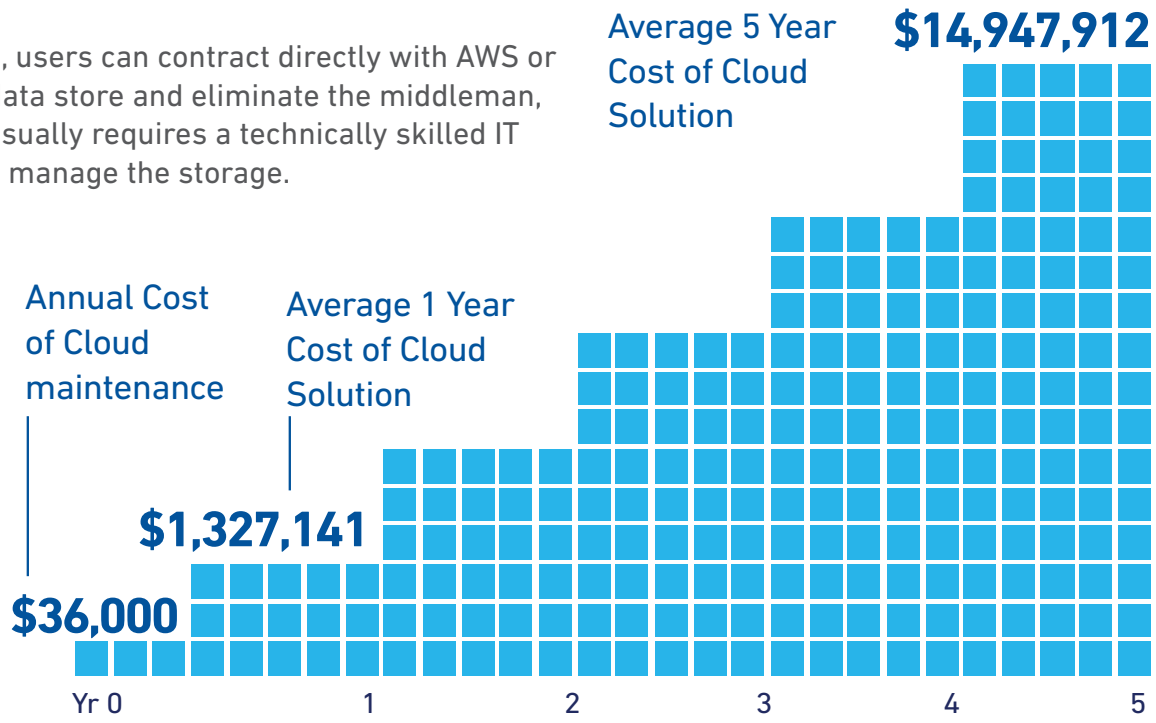
An agency that uses the vendor's video storage plan is locked in for the duration of the contract. Later, if they decide to change vendors, there could be a problem in transferring data from one storehouse to another, potentially forcing the agency to maintain two storage contracts to ensure access to their video data. If video is moved from one storage provider to another, the metadata scheme may be corrupted or lost, making the video difficult to catalog and index. In this case, metadata would include key information such as time and date, geographic coordinates, officers' names and identifiers, and any case information that had been coded into the file. Being tied to a single provider can also mean being at that provider's mercy if their storage fees rise in the future.

Of course, users can contract directly with AWS or another data store and eliminate the middleman, but that usually requires a technically skilled IT person to manage the storage.

Both approaches to online storage come with a large bandwidth requirement. The agency will be constantly uploading new video files to the cloud and retrieving video for review during preparation of reports and investigations. Many small agencies have no better Internet access than is available to the households in the communities they serve. That kind of volume can overtax the Internet service provider's network and/or result in excess data surcharges billed to the department.

Even when there is adequate bandwidth to handle an online-only storage strategy, the system is disabled when there is a failure of the data network. Public safety agencies in New Jersey suffered several such outages in 2015 when the Verizon network failed during a storm, isolating numerous offices from the data they required to conduct business.

Another data storage strategy uses a combination of local and online storage, balanced for the greatest possible efficiency. This is referred to as a multi-tier approach.



The high cost of cloud storage: Baltimore found out that the long-term cost of cloud storage was much more than anticipated.

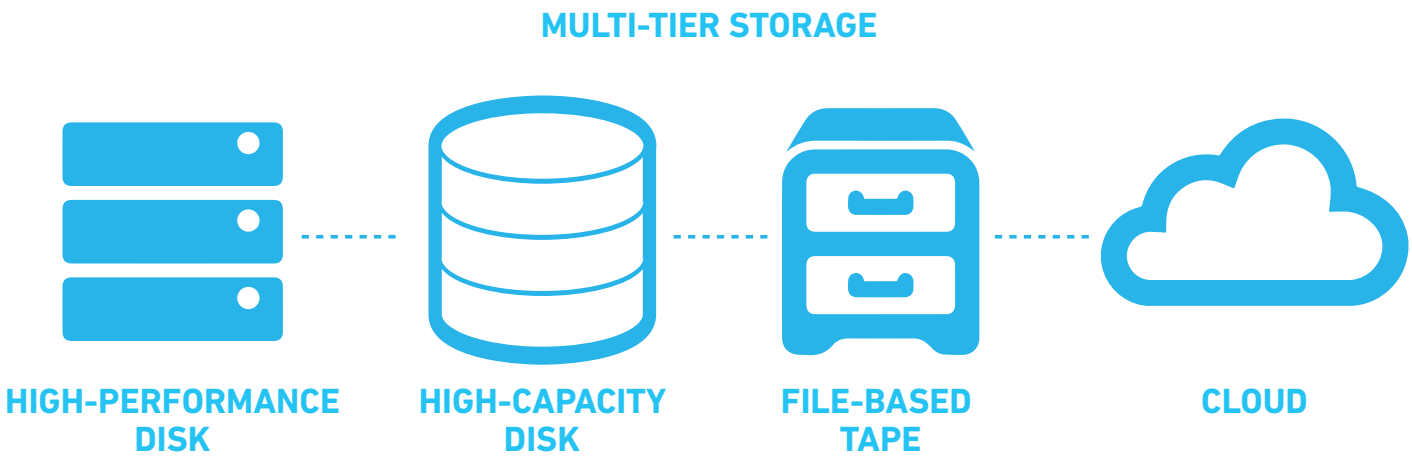
Option 3: Multi-tier storage

A multi-tier storage system combines different types of storage media, placing the most critical, high-priority data on the highest-speed devices and relegating files of lower immediate importance to slower devices that have a lower per-MB storage cost. These devices include:

- Solid-state disk (SSD), a store of memory chips with no moving parts. Access to data on these devices is very fast, but at a relatively high per-MB cost.
- Spinning hard drives, each with a capacity of up to several TB.
- File-based tape, which offers a much lower per-MB cost but takes slightly longer to retrieve data, compared to SSD or high-capacity disk.
- Cloud storage, used for disaster-proof backups may also be used for long term retention.

Software automatically manages and balances the different storage devices, placing files likely to be needed immediately on the faster media. As the files and the cases associated with them age, they are not accessed as often. This allows them to be moved to lower cost, higher capacity media, where they can still be retrieved in under two minutes.

A multi-tier storage approach may rely partially on a wide-area network connection for online storage, but only for backup copies and the lowest-priority files. A temporary service outage will not disable the system, as is the case when cloud storage is the primary medium.



Real-world solution

When the Calgary Police Service (CPS) launched their BWC program, they found their IT infrastructure would be quickly overwhelmed by the volume of video files generated by the cameras. The cameras were churning out 18.4GB of video per shift, and it wasn't long before the IT department would have to manage over a petabyte (1 million GB) of data.

The CPS had a retention policy requiring all video to be retained for 13 months. Files associated with a criminal case had to be kept for seven years, 20 years for a major crime, and 40 years if associated with a terrorism investigation. If they started using higher-resolution video or expanded the retention policy, the storage requirements multiplied.

The service had been using a scaled-up NAS solution for the video from their patrol car cameras, but expanding this to accommodate the BWC output was too expensive to consider. A multi-tier storage solution offered a savings of $300,000 per year over strictly online storage, with more convenient accessibility for the service's users. Using a multi-tier approach, they are able to manage over 4 petabytes of data with only 240TB of actual on-site disk capacity.

The result is faster, cheaper, more reliable access to video and other digital data without the need for a dedicated IT staff...

Summary

Multi-tier storage leverages multiple storage media types, using software that dynamically optimizes file locations by priority. The result is faster, cheaper, more reliable access to video and other digital data without the need for a dedicated IT staff to manage and oversee the process. The system is almost infinitely scalable, so much that few operations will outgrow it.

The most critical files are stored on-site, so a temporary loss of Internet service will not cripple the system. Offsite, cloud-based backups provide redundancy and disaster recovery. Even with those different types of media involved, the user sees the agency's data as if it was residing on a single drive, making data access easy and immediate.