EVIDENCE STORAGE: IN THE CLOUD OR NOT?

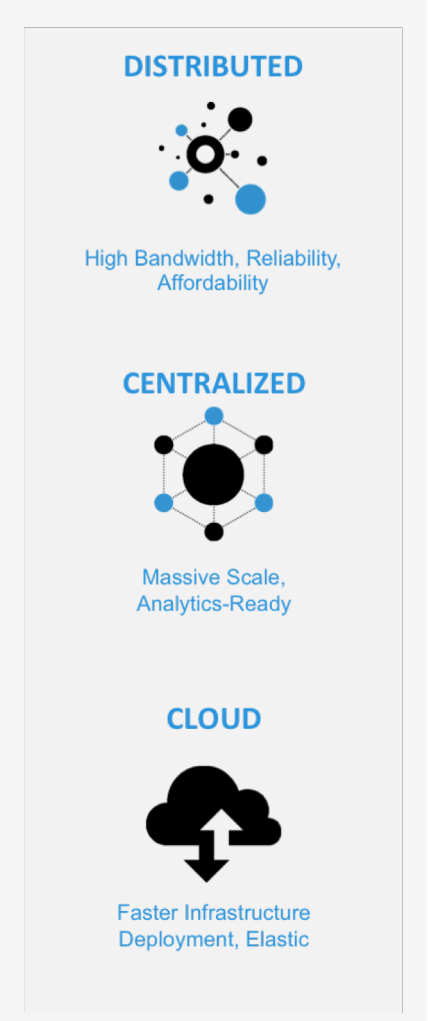
Navigating the on-premises vs. cloud surveillance storage landscape in Public Safety

On May 1, 2015, the Department of Justice announced a $20 million Body-Worn Camera Pilot Partnership Program to respond to the immediate needs of local and tribal law enforcement organizations. This Federal investment marks a significant push towards body-worn devices that will ultimately lead to a surge in video data. One third of these police departments are already using body cameras, and new departments are deploying devices every day. In order to scale to keep up with this "Video Vortex," organizations must decide whether to keep their data on premises or to go to the cloud. This is not a straightforward decision, or one that will be the same for every organization.

Every department has different requirements and regulations, and must understand both its options for storage architecture as well as the surveillance product life cycle before moving forward with a solution to fit its public safety needs. Choosing the right solution for *your* organization requires a clear understanding of the pricing implications associated with long-term storage, how quickly you will need access to evidentiary support, the product life cycle, and legislative storage requirements. This document will help you understand the differences in surveillance storage architectures and cost/product lifecycle considerations.

SURVEILLANCE STORAGE INFRASTRUCTURE

Storage is the foundation layer of any surveillance solution. However, many organizations purchase body-worn and other surveillance devices before they consider storage requirements or cost. This foundation layer must support an open platform capable of managing disparate data sets (from multiple devices) while addressing the challenge of scale head-on. It is important to understand the differences among the three major surveillance storage architectures—distributed, centralized, and cloud—and what option would be most suitable to your specific organizational needs and requirements.



Distributed architectures typically support several hundred surveillance devices. They store video and surveillance data locally and then periodically transfer the digital data set to the central platform. For example, a 'satellite' police station may store data locally in office, then periodically transfer it over to headquarters—the centralized location. Distributed architectures often integrate the data with applications and other systems, such as access control and intrusion detection, without engaging a central server. The resulting architecture reduces single points of failure and distributes processing requirements over many, smaller sites.

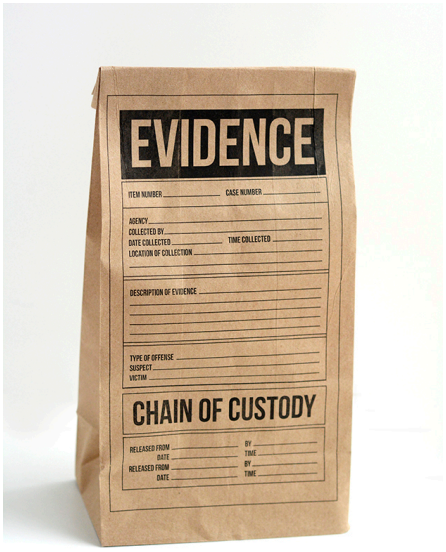
Scale is the primary consideration with **centralized architectures**. Commonly used by police headquarters, schools, Federal/government, airports, and energy companies, for example, centralized surveillance architectures host high camera- or device-count environments (typically thousands of surveillance devices) and are able to support large amounts of surveillance data. Storage must be made efficient and utilization rates must be high to prevent price creep, while migration time must be extremely low to non-existent to seamlessly apply changes in resolution or pixilation.

Many companies opt to go on-premises for their primary storage, but use **cloud architectures** for deeper 'cold' storage. Cloud provides an elastic storage platform that easily expands as data volumes grow. For surveillance-specific industries, this means expanding volumes in a centralized private cloud or even leveraging public cloud storage for more rapid capacity expansion. Ultimately, cloud storage can improve storage efficiencies and help reduce the costs associated with storing inactive data on more expensive storage solutions. However, using the cloud for surveillance data involves many different availability, security, and cost decisions.

SURVEILLANCE AND THE PRODUCT LIFE CYCLE

Storage requirements for surveillance and body-worn data differ widely from state to state, depending on the crime. Minor traffic stops may only need to be kept for 30-45 days, DUI's for over 3 years, and Federal crimes may need to be kept for many years or in some cases, indefinitely.

With more 13 million arrests each year—over half a million for violent crimes—body-worn data is adding up to a lot of storage. And because video from body-worn cameras will have a long shelf life, longer than that of any storage solution, organizations must think beyond 3-year or 5-year buying cycles and consider how they will manage/store this video for 25 years or more—on-premises vs. in the cloud.



Some vendors offer on-premises storage only, while some offer cloud-only storage. Some vendors offer cloud storage up front as a bundled offering with the cameras, enabling customers to go cloud first and then go on-premises to save on long-term cloud storage. While this bundled option simplifies the purchasing process, it may not be the best option for organizations with high retention requirements or who need to frequently move data from local to storage and back. Several body-worn camera manufacturers are bundling the device with cloud storage. Taser's Evidence.com cloud storage service averages $47 per user per month, while VieVu sells its cloud service as a bundle priced at $55 per month per officer. In comparison, onsite storage software bundles sell on average for $25 per officer per month[1].

How much storage will you need? Most departments will accrue approximately *one petabyte (PB)* of storage per year—which for example accounts for nearly half that of all US academic research libraries combined. With increasing device counts, retention requirements, and resolution upgrades being factored in, fast-growing storage and its associated costs will surely rise. Cloud costs are also variable and unpredictable in nature, whereas most on-premises solutions are fixed.

Going the pure cloud route, therefore, is not always the best option for public safety organizations. Choosing a vendor that offers both cloud and on-premises storage architectures is a better bet as it will safeguard an organization's assets while allowing for future growth. Many companies opt to go on-premises first with the bulk of their 'cold' or long-term storage, and then go to the cloud for deeper storage. This approach is often more cost-effective, provides greater security, and simplifies application integration.

WHY EMC?

Storage should be the very first consideration when looking at body-worn devices, as it is the most important—and costly—component of the overarching solution. As the industry's leading storage provider, EMC is in the business of building highly reliable, flexible, and secure data management environments with an emphasis on fixed versus variable cost, ownership of the data, better security, and the ability to integrate with other applications. EMC's open, hybrid architecture—built on both on-premises and cloud technologies—gives organizations the flexibility and scale they need to seamlessly scale their body-worn and surveillance solutions not only in the immediate future, but long-term as well as requirements and regulations change. It also enables organizations to manage data from a host of other applications like crime lab, digital evidence, surveillance, drones, in-car, license plate recognition, interview room rooms, crime scene footage, and more.

EMC will work with you to determine which surveillance architecture is the best approach for your organization's business objectives. Please contact us at Surveillance.Practice@emc.com for more information.

---

[1] Mearian, Lucas. "As Police Move to Adopt Body Cams, Storage Costs Set to Skyrocket." Computerworld. N.p., 3 Sept. 2015. Web. 29 Sept. 2015.