Verkada

Understanding Your Options for Extended Video Storage: **Local vs. Cloud vs. Hybrid Cloud**

Introduction

Video cameras come in many shapes and formats, but one common factor that unites them all is the amount of data they record and transmit. There are multiple means of storing and accessing this data, both locally on-premises and remotely in the cloud. Many industry leaders are forced to make cost and quality trade-offs when it comes to maximizing storage capacity on their cloud or local video recorders. Verkada's hybrid cloud storage model eliminates many of these limitations, allowing users to maintain the complete coverage that they need.

In this eBook, we'll explore the strengths and weaknesses of on-premise and cloud video storage, as well as how Verkada's hybrid approach combines the benefits of both for a predictable and consistent price.

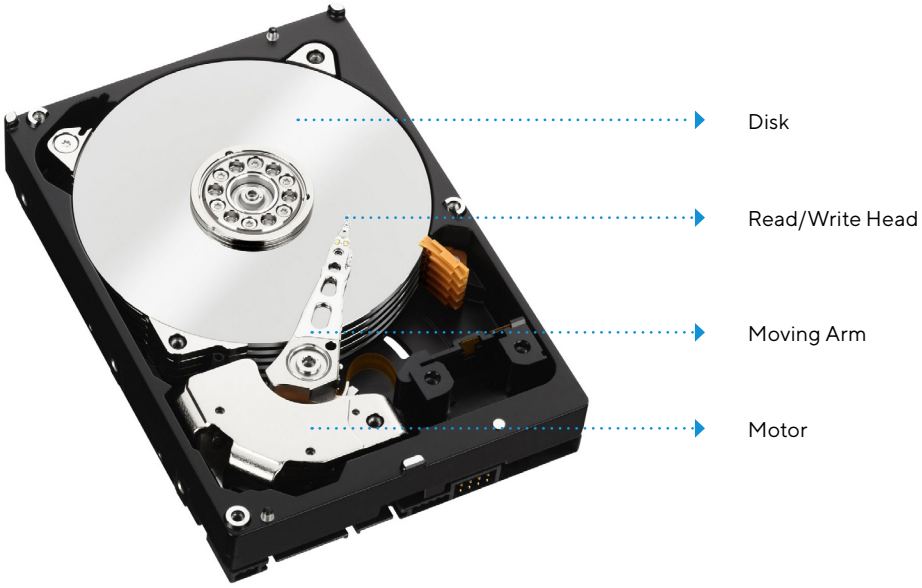
Limitations of On-Premise Storage (NVRs & DVRs)

Most NVRs store their footage on a group of hard disk drives (HDDs). If your organization relies on NVR storage, you may be interested in learning about the common myths and misconceptions many users have about their strengths and limitations. For Example, many organizations belive NVRs and DVRs offer the most reliable solution.

Reliability

According to a Backblaze study of over 25,000 HDDs running constantly for several years, hard drive failure occurs in three separate 'stages.' After a year and a half of use, 5% of drives suffered from mechanical failure. For the next 18 months, this metric dropped to around 1.5%. However, after the third year of use, an astonishing 12% of hard drives failed per year.

That means any legacy NVR system that has been running for six years likely has around half of its drives non-functioning and in need of replacement.



Above is an image of the inside of a standard hard drive. Small motors spin the disk (or platter) and move the arm so that the read/write needle head can make changes to data anywhere on the disk. These motors frequently burn out and stop functioning after constant and prolonged use. The read/write head is also vulnerable to mechanical failure, 'floating' only a few molecules over the disk itself. If the hard drive is tilted or jostled, the head and the disk might touch, causing irreparable damage to both components.

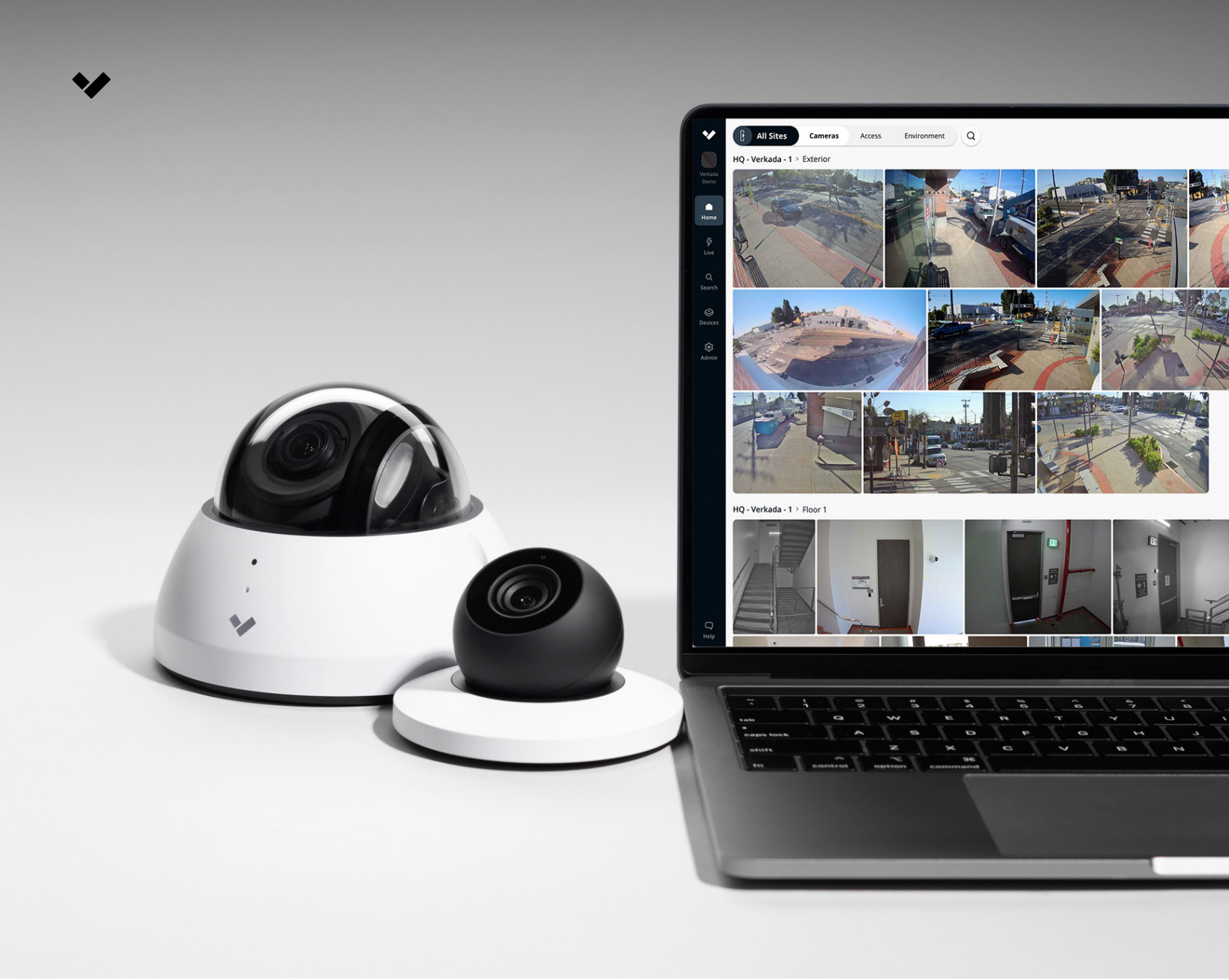
Data from a drive that has failed is in most cases irrecoverable, especially if the internal disk has been damaged. This poses a significant risk for organizations that are required by law or policy to retain video for a defined period of time. Hard drive failure-induced footage loss might result in punitive action or fines.

Limited Storage

The other issue that many NVR users struggle with is that of limited storage capacity on the devices themselves. NVRs and the hard drives they depend on have a finite amount of space that frequently forces organizations to make sacrifices on the performance and quality of their surveillance solutions. These sacrifices take various shapes and forms:

- **Image Quality:** High quality of footage is often the biggest culprit to a maxed-out NVR. Video storage size depends on a number of factors, including framerate, camera resolution, and the compression method used on the stored footage itself. In general, footage that is clearer, smoother and less pixelated takes up more storage space. In most cases, higher quality footage is more useful to organizations employing surveillance systems to capture faces, license plates, and other identifiable details. However, a finite amount of storage space means that these organizations must make a choice between storing lower quality footage and simply storing less footage. In many cases, surveillance installations that feature expensive 4K/8MP cameras don't even have the ability to store video in its native resolution without compressing it, effectively rendering these powerful cameras no better than their cheaper counterparts. When faced with the dilemma of insufficient storage capacity, many security stakeholders are forced to prioritize certain cameras that are placed in critical areas and continuously monitor feeds. This system of prioritization is ineffective at scale where there may be several subjective levels of importance.

- **Motion-Based Recording:** Another method of getting around the issues caused by a finite amount of storage is to only record footage when absolutely necessary. Monitoring camera feeds manually and only recording what is needed is infeasible, and would result in many missed incidents over time. For this reason, most modern surveillance cameras can be set to record when triggered by notable events like significant motion. These features are effective to an extent, but are inconsistent and plagued by false negatives. Making the choice between full hard drives and lost video is something of a catch-22, especially in cases that involve legal action or where missing footage is unacceptable.

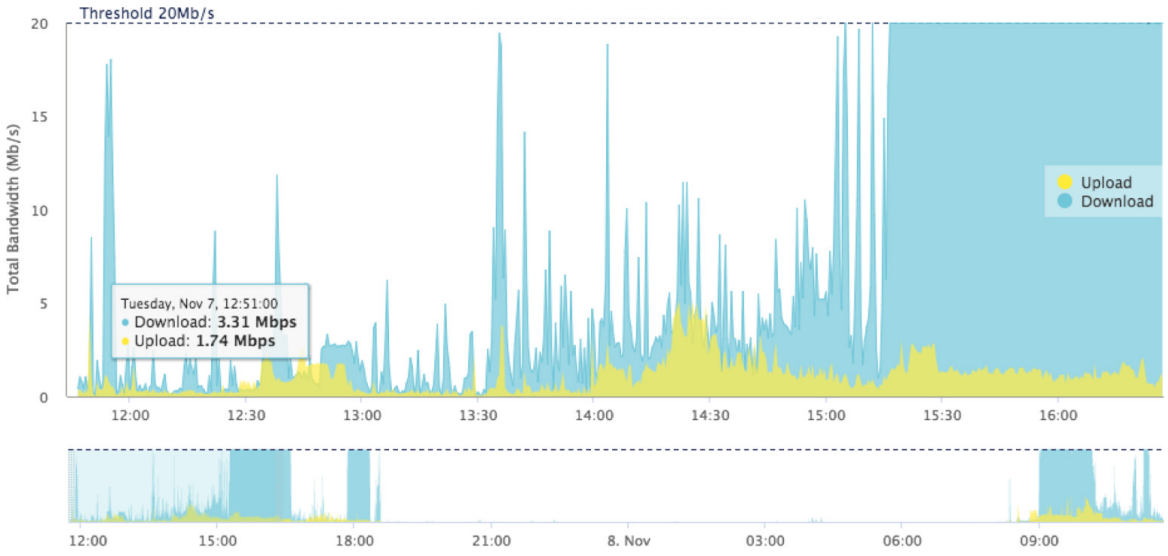


Limitations of Cloud Video Storage

Cloud-connected cameras solve many of the issues noted in the previous section. For example, digital storage on the cloud is effectively limitless, solving the issues caused by finite NVR storage. Similarly, cloud storage is almost always backed up redundantly across multiple servers, meaning that even in the rare case of cloud drive failure, footage will be safely stored in two or three different locations. That said, cloud cameras feature some unique problems related to their constant dependence on remote storage. These problems can be organized into three groups.

Bandwidth Usage

Certain cloud-connected cameras cameras stream footage continuously to the cloud, and as a result they consume a constant and sizable amount of bandwidth whenever they are active. The consequence of this constant traffic may be felt by all users who share the network, especially if cloud cameras are deployed at scale. The inadvertent result of excessive bandwidth consumption is often slower network speeds, lapses in network service, or even unpredictable overage costs.



This is an example of a network that has hit its bandwidth cap of 20Mbps. From around 15:15 onwards, users would experience slow network speeds, increased packet loss, and even dropped connections. When experiencing network overage, administrators are faced with a lose-lose scenario: either throttle network traffic which will impact the performance of both cameras and users, or purchase more bandwidth which may be impossible due to location or budgetary constraints.

Cloud Storage Costs

While cloud cameras are freed from the space limitations of unreliable and finite NVR hard drives, cloud storage is not a perfect solution to the problem. While the cloud effectively has limitless video storage capacity, every additional gigabyte of storage used incurs additional fees. A standard camera streaming in HD quality for 12 hours per day requires over 2.5 TB of storage per month, resulting in AWS S3 fees that total about $798 per camera per year*. Especially with large camera installations, these types of storage models can quickly become expensive. As a result, many security stakeholders make sacrifices to their cameras' performance in order to keep costs from growing exponentially. In effect, while the cloud theoretically offers the potential of infinite footage storage, administrators with budgetary restrictions are forced to make the same concessions to video quality and uptime as if they had an NVR with limited HDD space.

Network Outages

Due to the fact that cloud cameras immediately back up all footage to remote storage, they are completely dependent on proper network functionality. Any intermittent interruption to the network means that footage will not be backed up. If the cameras do not have access to local storage in this case, footage will be permanently lost. Lost footage might result in a dangerous lapse in compliance or an incident which is impossible to resolve. Likewise, with only one copy of footage that resides on the cloud, it is difficult to meet compliance standards without seperate dedicated on-site storage. In essence, you still require an NVR or DVR to ensure two copies of data.

*AWS S3 price claims based on S3 standard storage amount of 2.5 TB per month, and calculated with the AWS pricing calculator on March 9th, 2022.

Hybrid Cloud Storage: Solving Key Limitations of Local and Cloud Recorders

Verkada has implemented a hybrid solution that solves the major drawbacks of both closed-circuit NVR systems and cloud-connected cameras. Hybrid cloud architecture combines the reliability of local video memory with the limitless computing and storage potential of the cloud. The product of this novel combination is a video security platform that is dependable, resource-lean, and simple for the end-user to employ.

Reliability

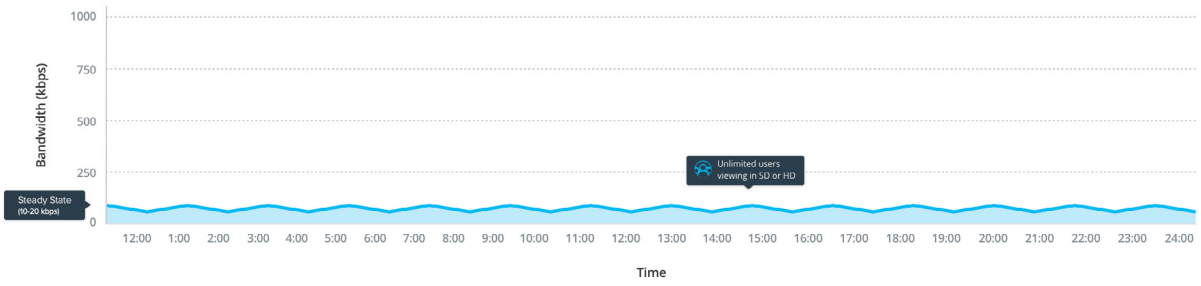
Because Verkada cameras feature built in high capacity solid-state drives (SSDs), storage is more reliable than that of legacy NVR solutions which use mechanical hard drives. Modern SSDs have been proven to be fail-proof for up to 300 TB of writing, depending on type and frequency of usage. In addition, configurable cloud backup ensures that when data is not stored locally, it is being protected by AWS's trusted servers and encrypted to AES-256. Reliability is one of AWS's five pillars of the Well Architected Framework, ensuring that data resiliency is integral to the ongoing operation of their cloud services. Read more about AWS's Reliability here.

Security

As soon as Verkada cameras are installed, they are protected by our industry-leading cybersecurity protocols, including multi-factor authentication, single sign-on, encryption of data in-transit and at-rest. These protections make Verkada products perfect for regulated industries, especially those who must comply with regulations such as PCI (Payment Card Industry) and HIPAA (Health Insurance Portability and Accountability Act) which require strict data protection protocols for footage. Unlike traditional CCTV systems, which are frequently plagued by unaddressed security vulnerabilities for months or years, Verkada devices are protected by an entire team of security experts and 3rd party penetration testers who seek out and patch vulnerabilities before they ever affect users. Verkada devices are designed to apply firmware updates automatically during off hours (to keeps bandwidth usage low). That means you'll never miss out when we roll out new features or critical security updates.

Network Efficiency

Verkada cameras are designed to make as minimal of an impact as possible on the network performance of the organizations they protect. A typical cloud-connected camera consumes about 1-5 Mbps of bandwidth when recording HD footage. In contrast, when in their default recording mode, Verkada cameras only consume 20 kbps. This makes Verkada Cameras much more practical to deploy at scale without affecting network bandwidth for other users.



The key to low-bandwidth is Verkada's unique hybrid cloud architecture. While recording normally in their "steady state" mode, Verkada cameras store footage locally to their solid state drives and only transmit thumbnails and metadata to the cloud. This approach allows users to intelligently and selectively stream only the footage they require at the moment. Additionally, for local viewers on the same network, streaming consumes no extra bandwidth— even when there are multiple simultaneous streams.

While Verkada cameras can locally store up to a 365 days of continuous video, the cloud license offers unlimited archiving in AWS. Because the cameras can continuously store footage during all hours, organizations can set their cameras to perform a backup during off-hours. This enables permanent retention of footage at scale without impacting network performance for other users.

Video Storage Options Infographic: Local, Cloud and Hybrid-Cloud

	On-premise Video Storage	Cloud Video Storage	Verkada Hybrid Cloud Storage
Overview	Traditional camera installations are typically connected via a wired or wireless connection to an NVR or DVR with attached low-cost hard disk drives.	Some modern camera systems stream footage data directly to the cloud using IP communications. This design eliminates the need for local storage and wired connections.	Hybrid Cloud installations combine onboard storage with the ability to back up footage to the cloud. This design combines the strengths of both cloud and on-prem storage.
Reliability	Most legacy NVRs rely on hard disk drives that are prone to failure due to mechanical parts that become worn over time, leading to data being irrevocably lost.	Footage is typically stored redundantly in the cloud, but network outages hamper uploads, potentially resulting in lost footage.	Secure SSDs and no single point of failure between local and cloud storage means that footage will not be lost, even in the case of network outage.
Storage Capacity	Variable amount of low-cost medium capacity HDDs, typically in multiples of 1 TB.	Virtually limitless, only constrained by price-per-GB rates and the user's budget.	15, 30, 60, 90, 120, or 365 days of local SSD storage with unlimited cloud archiving.
Scalability	Camera population is limited to the amount of ports available on the connected NVR/DVR.	Limited by available network bandwidth, anything more impacts performance for other users.	Not constrained by NVR ports, and low "steady state" mode only consumes a tiny amount of bandwidth.
Cost Considerations	Hardware frequently needs replacement, and upgrading camera coverage usually requires the purchase of additional recorders for extra data ports.	Cloud storage costs scale with usage and network bandwidth may need to be upgraded in order to support an expanding camera network.	2 line items: 1. Camera hardware – all models include a 10-year hardware warranty. 2. Command cloud software license – sold in 1, 3, 5, and 10 year contracts.
Final Takeaways	On-premise video is typically cost and labor-intensive to initially install, making it appropriate for organizations that want to upgrade existing NVR solutions. However, when it comes time to scale, costs quickly grow with the size of the installation.	Cloud storage is readily scalable, making it ideal for organizations that are rapidly growing. However, this comes as a trade-off at a increased cost for both storage and network costs meaning they require extra budget reserved for security.	The hybrid cloud model is reliable due to its combination of local and cloud storage. Its simple and expandable cloud license makes it ideal for smaller installations that grow with an organization's surveillance needs.