Breaking Through Legacy Limits with Wasabi Cloud Storage for Video Surveillance

Improving storage efficiency and security by combining on-prem and cloud storage technology

Safeguarding property and people. Analyzing traffic flows. Managing manufacturing production. The right approach to video surveillance can accomplish all of these needs. Organizations, both public and private, rely on video surveillance technologies to identify and mitigate risks, power new opportunities, drive incremental improvements, and improve outcomes for workers, citizens, and other stakeholders.

However, video surveillance is a complex collection of constantly evolving technologies under pressure from new requirements, demands, and expectations. Many organizations with substantial investments in video surveillance technologies realize, over time, that some elements of their tech stack interfere with their ability to cope with change. Data storage is one part of the technology stack that's under pressure -- with more cameras, higher resolution, and expanding demand for immediate data access, traditional video surveillance storage technologies might not get the job done.

Fortunately, there are ways to solve the problems where data storage is concerned. Leading vendors like Wasabi Technologies are leading organizations toward **superior data storage optimized for video surveillance** and proven successful under the most demanding conditions. In this paper, we'll explore the world of video surveillance, including trends and challenges, dig into storage pros and cons, and then take a deeper look at what Wasabi can do to support emerging, demanding video surveillance requirements.

HIGHLIGHTS

- Low price, high performance, secure object storage

- No egress or API request charges

- Quick uploads & downloads

- Data center redundancy

- 11x9s data durability

- Multi-Factor Authentication

- Robust partner network of leading video surveillance organizations

Understanding the Market Trends and Challenges

Video surveillance is a rapidly growing market. The global video surveillance system market was valued at USD 52.45 billion in 2020 and is expected to reach USD 90.37 billion by 2026, registering a CAGR of 9.31% from 2021 to 2026[1].

A nexus of trends and technology changes are powering and sustaining this growth. These include:
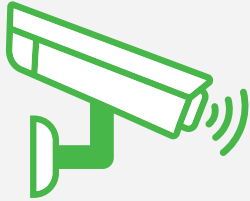
- New camera capabilities

- Expanding use cases

- Software is everywhere

- Cloud is universal

- Systems are more open

- Regulations are changing the game

1. New camera capabilities are enabling new possibilities.

If you ever saw a grainy, hard to view video surveillance screen, you probably already know that the industry has moved toward higher resolution video that captures more information, provides organizations with more clarity, and delivers additional value. The shift, over a decade, from SD-quality cameras to HD-quality meant that investment in video surveillance technology finally came into its own.

Now we're seeing a shift toward 8MP surveillance cameras, encouraging the capture of footage in 4K resolution. 4K has better imaging, better night vision capabilities, and more zoom value than Full HD (1080P) cameras. Those advantages matter to cost-sensitive organizations who can, depending on their requirements, deploy fewer cameras, avoid additional nighttime illumination, and gather details without expensive optical zoom lenses in their cameras.

The problem with 4k is simply that video surveillance data sets are much larger, due to the increased resolution. That data volume increase can put pressure on networks, compute resources, and data storage devices.

2. Use cases continue to expand.

When we think of video surveillance, we inevitably think of security. That's not surprising. When we see security cameras, we often see them in places (retail, commercial buildings) and applications (theft control and inappropriate access) that align with security.

However, when we think about security, there are areas of opportunity we often don't consider.

These can include:

- Schools, colleges, and universities. Schools and colleges use video surveillance in ways that go beyond traditional security concerns, including identifying the unauthorized shooting of videos on campus, bike and automobile accidents, fights, falling trees, thefts, cars using parking lots to "drift," vandalism, and more.

- Law enforcement: across the world, law enforcement agencies are adopting body-worn cameras and in-car video systems to enhance policing, improve public safety, and extend and preserve evidence.

- Military and border patrol: drone delivered video focuses on borders and provides invaluable information in conflict areas.

There's no question that security is a critical use case for video surveillance, but it's not the only use case. As video surveillance platforms become more affordable and add new features, unforeseen applications emerge. Some of these include:

Disaster response: fixed cameras and drone surveillance provide real-time information that helps firefighters and other first responders identify problem areas, locate and rescue people at risk, and plan responses more efficiently.

Smart Cities: city governments have cameras in thousands of locations, including sidewalks and street corners, giving them new ability to control traffic flows, send out notifications of traffic problems and delays, and obtain vehicle insights with license plate recognition.

Business operations: video surveillance provides a wealth of information for businesses to use, including opportunities to optimize manufacturing, respond to supply chain disruptions at loading docks and storage facilities, and even identify inappropriate actions taken by employees.

Healthcare: it's become normal to use video surveillance to monitor hospital patients and even record surgeries, but in the past two years, many healthcare providers, public health authorities, and even private companies added thermal cameras to help identify people with fevers, in an effort to reduce Covid-19 infection rates.

Residential properties: obviously video surveillance contributes to safety for both single-family and multi-unit residential facilities. But it's also commonly used to monitor the elderly and other vulnerable people, often in conjunction with sensor data.

In short, use cases continue to expand, providing new opportunities and new possibilities for individuals and organizations to improve safely, drive productivity, improve efficiency, and reduce costs.

However, there's a downside to this expansion. As more cameras are added, more live and recorded video streams exist. Using these efficiently and effectively becomes more problematic. Organizations that might have had only a dozen video cameras now have hundreds. That's why the next trend is so critical.

3. Software makes video surveillance better

All these use cases are made possible by a fundamental shift in how video surveillance data is used. If your first thought of video surveillance is a mental image of a security guard fast forwarding through recorded video, looking for a shoplifter, you're overlooking the most powerful tool in the video surveillance world today: software. Software innovations make video surveillance a game-changing tool for organizations because formerly impossible capabilities are now easy to get and easy to use.

The days of watching live feeds and occasionally rewinding video, looking for an event, are essentially over. Instead, analytics and artificial intelligence have become integral parts of the entire video surveillance industry. For example, today's retail security guard relies on software that offers situational awareness, offering in-depth insight into customer and employee behaviors, theft and trespassing, and store traffic patterns, to name a few applications.

Organizations using the right software, in the right way, discover that they can move from manual video surveillance (employees watching screens) to automated surveillance (AI-powered detection, alerting, and identification), giving them a powerful set of capabilities that transform the value of video surveillance. When people cause problems or events occur, the software can identify issues and let decision-makers know.

In addition, video content analytics (VCA) gives organizations a deeper understanding of any monitored dynamics. Imagine software that identifies a particular traffic pattern that only emerges on Fridays, or a pattern of shoplifting resulting from the arrival of a particular bus, and you can begin to gain some perspective on the power that VCA provides for organizations of all sizes. Rather than using video as a tool to identify problems in the past, VCA lets people discover possibilities for the future.

4. The cloud is ubiquitous

However, without another innovation, analytics would remain a capability that's limited to the largest organization. In the past, to get intensive video analytics, organizations had to put big servers and storage devices in their data centers, forcing them to swallow the downsides of high capital and operational expenses as well as dealing with high levels of complexity. Today, easy access to cloud computing makes powerful analytics, AI-powered insights, and even third-party integrations easy, safe, and cost-effective.

Cloud vendors know that flexibility and versatility are key to technology adoption, and they've made access to artificial intelligence and deep analytics easy, with pay-as-you-go, software-as-a-service models that easily scale up and down, with features that can be turned on and off (and billed incrementally) as needed. Analytics can be customized at a camera level, putting organizations in control of their capabilities and costs in an unprecedented way. Organizations no longer have the obstacles of high capital expense and ongoing operational costs and complexities -- instead, they have quick and easy access to deep video analytics that provide exponential value.

5. Systems are more open, making them more useful

Anyone with long-standing expertise in video surveillance remembers the days of closed, proprietary systems that offered end to end capabilities from a single vendor. Today's situation is very different. For years now, vendors have understood it isn't fair to deny organizations the ability to build out a custom video surveillance solution, combining the best-of-breed technologies, to fit their specific situations and needs.

Open standards like ONVIF[2] set the stage for assumptions that compliant products would simply work together as a functional solution. Bodies like the PSIA[3] have played a critical role in determining how video surveillance devices and software interoperability functions in real-world environments. Organizations and security integrators have come to expect that video surveillance technologies will be as simple as the "plug and play" interoperability we take for granted with our computers, smartphones, stereo systems and more. Basic steps, like standardizing on IP protocol, made all the difference.

Thanks to all these interoperability and open standards efforts, customers have choices at any level of a video surveillance system -- from cameras and networks to screens and software. Those choices drive down costs, foster competition, and ultimately make solutions better.

6. Regulations are putting new pressure on video surveillance

As all of us watch television, movies, and TikTok(™) videos, it rarely occurs to us that video is an area that's attracted regulatory scrutiny. However, literally thousands of laws exist that impact requirements around video surveillance. It's not just that laws exist that govern camera placement, but laws and regulations exist at municipal, state and federal levels that govern different video retention requirements for different types of video for different use cases. For example, in Georgia, video created by cameras in a police vehicle or by a camera on a police officer has to be retained for 180 days, while in Illinois, the same types of video have to be retained for at least ninety days and a maximum of two years[4].

Other environments, like healthcare, have their own requirements. Under HIPAA, video in healthcare settings is often considered protected health information (PHI), and as such, may have the same retention requirements as any other medical record. Requirements vary -- federal regulations require PHI to be protected for five years, while AHIMA recommends ten years. Thanks to retention policies like these, hot data -- recently created and relatively "likely to be used" data -- consumes a relatively small proportion of the total video surveillance data set. In typical deployments, 75-90% of the total utilized storage capacity is devoted to archived video surveillance data.

To make matters worse, regulations change all the time. The trend is for longer and longer retention times, meaning that over time, we can expect regulations to accelerate the compounding growth of data, increasing a "fear of deletion" mentality adopted by many organizations

Data. That's the key consideration at play here. We have more cameras, higher resolution, more use cases, and longer retention periods coupled with more ease of use and simplicity around standards, meaning that organizations simply have more data to collect, store, utilize and retain. Today's video surveillance data sets are being measured in terabytes, and tomorrow organizations will be collecting, storing, and analyzing petabytes of video.

All these trends and considerations point to the need to rethink data storage. It's becoming clear that some data storage platforms don't align well to the emerging trends, technologies, and shifts in utilization we've just addressed -- and organizations are beginning to encounter problems in data collection, data access, and data protection that interfere with the value of video surveillance, impede operational effectiveness, and even cause legal and regulatory issues.

Trends in Video Surveillance Storage

To cope with changes in data growth, data utilization, and data retention, organizations essentially have three choices for data storage.

- **On-premise storage** -- the traditional option.

- **All cloud storage** -- an option for smaller camera installations.

- **Hybrid storage** -- the leading-edge possibility.

Let's begin by exploring on-premise storage. If you evaluated video surveillance systems a decade ago, nearly every system came with on-premise storage or required on-premise storage. Whether on-premise video surveillance storage consists of several proprietary video recorders or some type of centralized, networked storage, on-premise storage has its weaknesses that limit operational effectiveness, including:

1. **It can be expensive to procure.** Traditional on-premise storage is typically purchased as a product, requiring capital investment and the need to manage both financial and operational depreciation over time. Spending hundreds of thousands of dollars on a video surveillance storage solution can simply be out of reach for an organization, or an organization may simply not want to allocate a large portion of an annual IT budget for a single requirement. On-prem storage often costs 30% of an entire video surveillance solution, and that's too much -- blocking opportunities to improve the solution, add cameras, increase frame rates or resolution.

2. **High ongoing costs.** On-premise storage comes with ongoing costs, including power and cooling, maintenance and updating, installing drive upgrades.

3. **It can be at the wrong location.** If you need on-premise storage at one site and you have available capacity at another location, that capacity may not be usable. It's not uncommon for some sites to need more storage while other sites have excess capacity.

4. **Delays in time to value.** There's a significant gap between purchase time and bringing a new storage system online, especially in these days of supply chain constraints. Organizations rarely want to wait weeks or months to bring a new storage platform or expansions to existing platforms online.

5. **The need for specialized expertise.** On-premise storage requires on-premise administration and maintenance. It can be hard to find dedicated storage administrators on the video surveillance side, and so it's often a time-consuming, "second hat" job for someone who is stuck doing administrative tasks: updating firmware, adding drives, conducting rebuilds, sitting on technical support calls. If an organization has dozens or hundreds of locations, on-premise technical administrators are likely to be in short supply and they'll struggle with the need to manage dozens or hundreds of consoles without a unified view.

6. **Scale limitations.** On-premise storage platforms have capacity limits. If you want to add more cameras, more resolution, or longer retention, storage infrastructure may simply be unable to cope.

7. **Limited security and resilience.** Many on-premise storage devices have limited built-in resilience. They probably can withstand a drive failure but might lack integrated multi-site data protection, automated backup or disaster recovery, and may not even support immutable data volumes to defend against threats like ransomware. They're also potentially insecure -- it's easy enough to steal a video recorder or rip drives from a storage device, leaving potentially confidential data vulnerable.

8. **Support limitations.** Most storage products come with a three to five-year warranty. However, extensions can be costly or simply unavailable after the warranty period expires.

9. **Technical debt** -- over time, the storage infrastructure may become more and more limiting as new opportunities and technologies arise. Ultimately, on-premise storage can become an obstacle to innovation.

> "Footage was held for a minimum amount of time, but after that, we had to let it go in order to save storage space. Now, instead of deleting those files, we are pushing them to Wasabi for maximum storage time, which is exceeding our retention expectations."
>
> **- Aaron Miller, Director of IT, Hardin County Government**

Due to these challenges, many organizations are trying to work out ways to augment and extend their on-prem storage. An obvious step is to evaluate and adopt cloud storage, and to be frank, cloud storage comes with compelling advantages compared to traditional on-premise storage. Organizations using on-premise storage often reach an inflection point where they discover that their platform, which was once fit for purpose, now impedes their ability to expand, augment, and improve their video surveillance infrastructure.

Organizations who:

- Have storage that's at 80% utilization

- Have storage that's no longer under warranty

- Have storage that's at the end of a depreciation cycle

- Have ongoing storage reliability problems

- Need lower cost solutions

- Have new needs to fit new solutions, or expansion requirements…

Are likely to consider a shift to cloud.

The advantages of cloud storage include:

1. **Cloud economics.** Instead of substantial capital expenditures, organizations can access storage via a "pay-as-you-go" model that reduces budget impact.

2. **Better operating expenses.** With cloud storage, there's no need to pay for power, or cooling, or ongoing repairs, or ongoing updates or warranty costs or rip and replace costs.

3. **Simplified operations.** Admins have centralized control over all storage volumes, aren't as challenged and don't have to visit location after location.

4. **Faster deployment.** Cloud storage can be turned on for any location, at any time, without any delays.

5. **Scale and flexibility.** Cloud storage can scale in moments, there's no need to add expansion enclosures, run cables, purchase larger drives, and expansion capacity is essentially limitless.

6. **Cloud is future proofed.** Cloud vendors update infrastructure as needed with seamless migration that's managed by the cloud provider. There's no technical debt or feature restriction.

7. **Resilience.** Cloud is intrinsically highly secure, highly protected, and ideal for organizations concerned with compliance, security and privacy issues.

For these reasons and many others, organizations often find themselves transitioning to cloud storage as a compelling way to get more capacity, at a lower cost/TB, without the costs of a rip and replace on-premise upgrade.

But to be direct, a full-fledged shift to cloud storage can come with problems. It's a complete architectural change that may require substantial software and workflow modifications. Migrating data to the cloud can become complicated and costly and risky. Not all clouds are the same, not every type of cloud storage is optimized for video surveillance, and it's not uncommon for cloud storage to contain hidden costs (API calls, egress fees, storage tier fees) that result in unpredictable spend over time, and increased total cost of ownership. Finally, cloud requires a new set of skills which might be in short supply within an organization.

As a result, it's becoming increasingly common for organizations to choose a path that tries to strike a balance between the advantages of cloud and the complexities of a full-fledged cloud migration. Leading-edge organizations are increasingly adopting a hybrid approach that mixes on-premise storage with the benefits and capabilities of the cloud. Rather than the one-size-fits-all approach of migrating everything to the cloud, a hybrid cloud approach offers a tailored mix of features, functionality, and benefits designed for the skills, opportunities, restrictions and limitations of a particular organization.

A hybrid cloud solution uses a combination of both on-premises and cloud technology, mixing and matching capabilities as needed. For those that are still content with their current on-premises deployment but are planning ahead, those who are getting somewhat frustrated with on-premise storage but want incremental change over time, or those who genuinely see the value of a mix, keeping fresh video local and sending older video the cloud, hybrid cloud approach gives organizations a compelling set of advantages, including:

- The ability to move at their own pace, incrementally, rather than be forced into an end-to-end transformation

- A way to increase recording criteria (frame rates and resolution) without costly on-premise expansion and upgrades

- A way to increase retention times without costly on-premise expansion and upgrades

- A way to avoid costly, complicated, risky migration

- A way to support new locations without new, costly, on-premise storage

- Added versatility: upload to the cloud when convenient, use the cloud as a backup or disaster recovery tool, provide remote access to videos if needed to support multiple locations, or provide third-party access to data

- An opportunity to continue leveraging on-premise storage until it's fully depreciated or out of warranty.

- A straightforward approach to reducing $/TB over time.

- An easy approach to improving security profiles over time.

There's a tendency to think that just because someone is a market leader, all their technologies are best-in-breed -- and that's simply not the case. For a specialized solution like video surveillance, some cloud providers are better than others.

Discovering the Right Storage for Video Surveillance

So if we begin with the premise that some cloud providers are better for video surveillance than others, what are the key criteria for picking an optimal solution?

1. The pricing model has to be optimized for video surveillance. Not every kind of cloud storage is. There are no data download fees (egress), no transfer/migration fees, no extra costs for long-term retention, no API fees, pay-as-you-go scalability, etc.

2. It has to be performant -- no hard limits on ingest rates, high bandwidth, high drive performance. It's also essential that performance doesn't degrade over time as total storage consumed increases.

3. Storage has to be instantly accessible -- some cloud storage offers SLAs measured in minutes or hours; ideally any video surveillance stream should be accessible in seconds from any location.

4. The storage has to support a widely supported API for key use cases like backup, archive, and analytics. Supporting a standardAPI also facilitates use in complicated hybrid cloud environments where data transfer from one cloud to another could be a necessity.

5. It has to be inherently resilient, with multiple layers of data protection, downtime protection, and disaster protection.

6. It has to support the highest physical and digital security levels to support regulatory compliance requirements and be well-positioned to adapt to regulatory changes. It should support ways, beyond access protection, to ensure that your video surveillance data can't be encrypted, modified, or deleted by bad actors or threats like ransomware.

7. It has to be easily purchased, provisioned, managed, and maintained.

The reality is that some of the leading cloud storage providers can't quite match these criteria. For example, the most prominent vendor has a complex pricing structure that includes a variety of charges that depend on utilization, requests and data retrievals, data transfers, management and analytics, and replication[5]. Costs are unpredictable and become more unpredictable as data sets grow, data access requests increase, and new regulatory pressures emerge.

Fortunately, there is a cloud storage platform optimized for and ideally suited to, video surveillance.

The Wasabi Way

Wasabi is a leading provider of cloud storage for enterprise video surveillance requirements. It's aimed at disrupting incumbent pricing and feature models with a powerful mix of enterprise-grade capabilities, singular focus on video surveillance needs, and an emphasis on simplicity. It meets or exceeds all the critical criteria for an optimized video surveillance storage platform. Wasabi delivers:

1. **Disruptive cost savings** -- as much as 80% less than a leading provider -- as much as 80% less than a leading provider -- with pay-as-you-go scalability and no hidden fees for data transfers

2. **Powerful security** -- not only does it offer leading-edge physical and digital security, for video surveillance, but your administrators can also make their storage immutable -- write once, read many, change nothing -- for a user defined retention period. For regulatory video retention, this single feature solves many problems!

3. **Compelling performance** -- no delays on retrieval. Wasabi provides instant accessibility for any video stream you store.

4. **Ease of administration** -- one global management tool for all your video surveillance storage functions, worldwide, that facilitates cost-effective management and data utilization, including analytics.

And unlike other cloud storage products, Wasabi enjoys strong partnerships with video surveillance technology alliance partners who can help craft or enhance video surveillance solutions that get the most value out of Wasabi.

To put this into perspective, Wasabi conducted a cost comparison[6] that evaluated a closed ecosystem, single vendor solution vs an open system purchased through a partner, with Wasabi cloud storage. The analysis proved that the closed solution storage costs were $350,000, while the Wasabi solution storage costs came to $36,000 over five years. That budget savings could be allocated to adding more cameras, increasing retention policies, or investing in other requirements. Or, to put it another way, the cost savings from using Wasabi could make a business more efficient, effective, or versatile.

Wasabi hot cloud storage offers a compelling way forward for video surveillance solutions. To learn more about Wasabi for video surveillance visit www.wasabi.com/surveillance

www.wasabi.com

End Notes

1   https://www.mordorintelligence.com/industry-reports/global-video-surveillance-market-industry

2   https://en.wikipedia.org/wiki/ONVIF

3   https://psialliance.org/

4   https://theboringlab.com/video-retention-requirements-law-enforcement/

5   https://aws.amazon.com/s3/pricing/?p=pm&c=s3&z=4

6   https://wasabi.com/surveillance/

7   https://wasabi.com/resource/hardin-county-case-study/