The Benefits of a Hybrid-Cloud Architecture For Video Surveillance

A comparison of Hybrid Cloud, VSaaS, and “Build your own cloud”

Table of Contents

Executive Summary

There is a lot of hype around the theory that cloud services are a less-expensive option for video surveillance. In many cases, this is simply not the case. When projecting the cost savings from using the cloud for surveillance video storage, the deployment model that you implement will make an impact on the cost over the life of the solution. Different architectures have significant cost differences. Vendors price their solutions very differently. For example, VSaaS services offer a choice of purchasing with a subscription like model. Some Video Management Software (VMS) vendors offer build-your-own-cloud blueprints, and a hybrid cloud architecture combines both on-site and cloud functions. There are significant differences in all three cloud implementations, so it's important to make sure that you are comparing apples-to-apples when investigating which is right to you.

Weighing the options

There are many reasons for security operations to move from centralized on-site video storage to a cloud model. For example, the cloud is infinitely more scalable and durable than on-site solutions. However, the most compelling reason that organizations are interested in the cloud is economics.

But when organizations move from on-site to cloud, do they really get the cost savings that cloud storage is known for? The answer is… it depends. There are different ways to incorporate cloud services in surveillance, and the one you choose will have a significant impact on your cost savings. So how do you make the best choice?

VSaaS

Cloud based video surveillance services, also known as Video Surveillance as a Service (VSaaS) is a niche market that is steadily growing. They are attractive to organizations because they offer the promise of a reduced burden of managing physical security infrastructure. While the adoption of VSaaS is already common in residential and small business environments, it is increasingly being considered as an alternative to traditional on-site surveillance for larger organizations and enterprises with multiple sites to manage.

Most VSaaS providers offer subscription-based prices on a per-camera basis. The prices range based on frame rates and retention period. In most cases, you can't repurpose the cameras you already own or choose cameras from other vendors that offer the features you like. You must use the cameras that are provided by the VSaaS vendor. That's because these cameras are small recording servers. They must contain enough storage and intelligence to buffer camera data during an internet outage. Keep in mind that their price is substantially higher, and the quality and/or features available may fall short of your expectations.

Another challenge associated with the VSaaS model is that for some, data is not stored locally. It is streamed directly to the cloud then back to the viewing station. In the event of an internet outage, the individual cameras will continue to record, but security operators will have nothing to review. They will not have access to "live" data. Worse, in case of a catastrophic event, where the internet goes down for days, public safety officials and relief agencies will have absolutely nothing to work with.

VSaaS providers have begun providing advanced analytics capabilities, such as facial recognition, object tracking, and license plate recognition. However, these capabilities are not part of the standard set of features and these "add-on" services are usually very expensive and vendor specific, they don't give you a full range of options or the ability to pick a best-of-breed analytics application vendor.

There is a reason VSaaS are most often found in residential and small business environments. It is a good model where only a handful of cameras must be deployed at many locations. However, it presents serious weaknesses for critical environments where lots of cameras are found and the need for more complex integration of other on-site physical security systems arise.

Build-your-own cloud

Some VMS vendors offer you blueprints on how to run their platform and software add-ons in the cloud yourself. This "lift and shift" method is borrowed from the IT world where it has had mixed results for the past 10 years.

Having an option to deploy your choice of VMS in a public cloud makes it easy to find, buy, and manage software and services. By deploying it from a cloud Marketplace you save time on system set-up with automated OS and VMS installations, and a pre-configured VMS.

In such a full-cloud deployment scenario, the cameras and the end-device used to access the system make up the only hardware maintained on-premises. The servers, recorders, and data centers are maintained fully by public cloud providers 24/7, anywhere in the world.

Popular VMS vendors such as Milestone, Genetec, and Avigilon offer a user-experience identical to on-site with 100% feature compatibility.

The value of cloud for surveillance (why cloud in the first place)

- "Cloud Economics"
- Reduction in operational costs
- Simplified operations
- Scalability and flexibility – future proof
- Video file protection

Hybrid-cloud architecture

A hybrid model is achieved when the existing hardware infrastructure remains intact, but the local storage is seamlessly extended to the cloud using a software gateway. With a hybrid approach to video surveillance storage, you can get the best of both on-site infrastructure and public cloud services. By combining both, you can mix and match where you store your data to best suit your needs.

Hybrid cloud is becoming more common in the Information Technology world and has significant advantages for surveillance video storage, especially for medium to large installations. These advantages include:

- Investment protection of existing endpoints, servers, and VMS and applications.
- Open architecture allows for a best-of-breed technologies throughout the infrastructure and the ability to adopt new technologies quicker

- Minimal amount of hardware that organizations physically have to own and babysit.
- Organizations can copy all local recordings to the cloud for backup purposes to protect against local hardware failure, file corruption, malicious destruction.
- The cloud copy can be used for remote access to videos. It can be easier to access them from the cloud than from local storage.
- The cloud is often safer than on-site storage.
- Scalability on demand: If an organization adds more cameras, increases resolution, increases frame rate or activity, or lengthens the retention period, they don't have to buy more hardware.

With a hybrid approach, you can upload video files to the cloud when it's convenient—such as after hours when your network is free of other traffic. And in the event your internet connection goes down and you can't reach the cloud, you can continue business operations with the video data you still have stored on-premises.

Cloud and on-site solutions offer different benefits, and organizations today leverage both. Hybrid cloud allows you to easily take the best of both worlds – own your data and rent the cloud, as needed. If an internet outage occurs during a catastrophic event, the hybrid approach is the only one ensuring ongoing recording, viewing of all live cameras, as well as instant access to at least 2-3 days of locally buffered recordings.

Six "Gotchas" to be aware of

Don't overpay

You need to also determine whether there are any hidden costs. How will you purchase your cloud storage? Will you buy it yourself, and therefore get the best price from the cloud vendor you select? Or is the storage cost hidden in a VSaaS subscription. Many VSaaS vendors build their service on hyperscaler clouds, mark up their cost and pass them onto their customers. The customer doesn't realize they are overpaying because of the way the subscription is billed.

We've seen examples of this before. Over the past few years, articles have been published exposing some body worn camera services that were accused of gouging law enforcement agencies. They buried storage charges that were up to ten times higher than typical storage costs. Law enforcement agencies and taxpayers were locked into multiyear contracts and had no way to extract themselves.

First generation cloud storage from the big three cloud providers (Amazon, Microsoft, Google) have a number of additional costs and transaction fees that make total costs unpredictable and difficult to calculate. Beyond the capacity-based charge for storing your video files, these cloud storage providers make you pay to access, move, or inspect your files. Those hidden fees not only add substantially to your overall costs, depending on the cloud storage tier you use, they can be more expensive than your storage cost.

Know who owns your video surveillance files

When the business relationship is directly between you and the cloud storage provider, it is very clear who owns the video files… you do. However, if the VSaaS vendor has the business relationship with the cloud provider it is not clear. Does the cloud provider acknowledge you as the owner or the VSaaS vendor? The cloud provider may view them and not you as the owner of the video files. If that is the case, then what happens to the video if the VSaaS vendor goes out of business or is acquired? In that case, you could potentially lose all of your video.

If the VSaaS vendor uses its own cloud, it is critically important to read the fine print and Terms of Use. Using body camera services as an example again, Law Enforcement agencies were shocked to learn that their Part of the Terms of Use included a clause that gave their vendor irrevocable and royalty-free rights to all the video on its server. The notion that private companies may be in a position to maintain the rights of this footage should raise significant alarms with the municipalities and public safety organizations who contract with these companies. Security and surveillance organizations considering VSaaS should carefully review the terms of agreement to ensure there are no loopholes which would allow companies to maintain the rights to the footage.

Avoid vendor lock-in

When choosing a cloud solution, it is important to be sure that you are not locked into a single vendor. VSaaS solutions tend to be “closed environments” that limit your ability to choose the add-on features that best meet their needs. A hybrid cloud architecture gives you more options and flexibility for deploying new edge devices, analytics, VMS and add-ons in a way that makes the best use of your changing requirements and the budget you have to work with. VSaaS often prevents organizations from rapidly adopting or switching to emerging or state-of-the-art tools that can improve your services and increase security.

“Build-your-own all-in-the-cloud” is often a mistake

For many organizations, a transition to the cloud seems inevitable, especially when their executive leadership has been hearing about the value of cloud for the IT side of the house for the past 15 years. Perhaps surprisingly, many actually cite cost as the key incentive for using public cloud, despite the fact that, in many cases, it is significantly more expensive than on-site surveillance solutions. Predictable workloads such as running a VMS, recording servers, and storage, on average were about twice as expensive to run in the cloud as compared to on-site. For spin-up and spin-down, burstable workloads, public cloud services are a good option. But video surveillance workloads are persistent and predictable, and thus are usually far more efficient and economical to run on-site.

The first hurdles to overcome in a build-your-own scenario are to provide adequate resources, guidance, and time to bring staff up to speed on the various required cloud services. Most organizations do not fully consider the investment necessary to properly staff for cloud expertise including cloud security, cloud databases, cloud networking, and cloud computing.

Thanks to highly complex pricing models, many organizations that adopt a build-your-own architecture suffer “sticker shock” when their monthly bill arrives. It’s important to understand the potential for hidden costs for “transactions”, overhead, video retrieval, and network bandwidth when utilizing some public clouds. While per-unit costs may appear trivial, they add up quickly and make predicting cloud bills next to impossible.

Lessons learned from the IT side of the house

The corporate IT and data teams have been migrating applications to the cloud for the better part of the past 15 years and there are a few things we can learn from their successes and failures. There are a few situations in which we've seen them move some or even all of their infrastructure back to an on-site data center.

The first, is that the camera data must make it to the cloud in the first place. An especially troubling challenge is that even temporary performance issues and network outages result in lost camera data. Period. And that's the one thing that a VMS should never do – lose camera data. It is possible to alleviate the occasional outage by attaching a memory card to each camera, but that is only viable for short outages (and these cards must be replaced quite regularly).

And much like with the VSaaS model, the solution becomes totally useless during any prolonged internet outage.

Second, is that if your public cloud expenses have grown beyond what an on-site solution would cost. Steady workloads, such as video surveillance, are usually less expensive to run on-site.

Third, it is far easier to control for compute performance and troubleshooting on-site than in the cloud and doesn't require all new skill sets.

Fourth, workloads, such as surveillance, that require low latencies or that transfer large quantities of video over the network are also prime candidates for repatriation, as network transit costs can make up a significant portion of a cloud bill.

The best times to consider a move to the cloud

There are basically five triggering events that can drive an opportunity to incorporate cloud storage into your surveillance infrastructure.

- **Near the end of your storage array's depreciation cycle**
- **When you've reached maximum storage capacity**
- **Your storage is no longer under warranty**
- **Application performance demands exceed storage array's capabilities**
- **Storage array is at the end of life**
- **New projects bring additional storage requirements**

Plan your video retention strategy

It is important to have a plan for your long-term retention and archival needs. For many organizations, legal compliance and industry regulations dictate the need to retain video files for possibly years. As video archives grow over time, so do the costs to store them. The temptation to leverage "cheap and deep" cloud archival storage such as AWS Glacier is powerful. Although Glacier and other "cold storage" tiers offer attractive per TB pricing, they are loaded with hidden charges that can break your budget. The cold storage tiers have additional charges for each video file you store in them. You are charged each time you do routine inventory management, integrity checks, and download your video.

Additionally, cold storage has a notoriously slow retrieval time. The retrieval process can take anywhere from three to 15 hours to return your video. This can have significant implications for organizations that are interested in using analytics on video surveillance. Forward-thinking public safety departments can build data lakes from pools of video feeding from different sources, such as in-car video, video cameras,

body-worn cameras, and drones. From this pool of videos, analytic applications can be used for object and facial matching, anomaly detection, license plate reading, and crowd counting. If the analytics application gets a "hit" on its metadata search for a person of interest or suspicious behavior, waiting up to 15 hours to access the relevant video file will be unacceptable.

At the other end of the spectrum, many organizations have short term retention requirements. Public schools, retail stores, and multi-tenant office buildings are used to deleting video files within 30 to 60 days. Many low cost "warm" and "cold" cloud storage tiers have minimum chargeable retention periods of 90, 180, or even 365 days. You can delete your video sooner than the periods specify, but you will be charged for the full period, thus negating the savings from lower storage costs and will often end up paying more than "hot" cloud storage alternatives.

Security and Protection Concerns

Recent headline news of the hacking of a major VSaaS vendor has exposed the security risks of some VSaaS architectures. All of the customers of Verkada, a VSaaS company, were compromised when a group of hackers gained access to 150,000 video cameras and archived footage. Video footage from organizations that focus heavily on security such as hospitals, schools, Fortune 500 companies, police departments, and prisons were compromised.

It's one thing to make sure the actual camera is secure (live stream), but it's another to make sure the storage of that video, in transit and at rest, is secure. In the case of Verkada, both were compromised. A hybrid cloud solution that utilizes an VMS on-site, while "air gapping" the archived video files in cloud storage, is the first step in establishing effective protection for your surveillance video footage.

With a hybrid cloud architecture, you can implement video file immutability to ensure the highest level of security for surveillance footage. Immutability protects against accidental or malicious data destruction. An immutable video file cannot be deleted or modified by anyone—including the cloud service provider.

When you create a cloud storage bucket (the basic container that holds your video and data) you have the option of making it immutable for a configurable retention period (in increments of days, weeks, months, or years). If desired, you can also configure the storage bucket to automatically delete the video after the retention period has expired. Video files written to that bucket cannot be deleted or altered in any way, by anyone, throughout its storage lifetime.

In addition to Immutable buckets, make sure that your cloud storage provider takes a "defense-in-depth" approach to security to protect against the widest range of threats. Choose a cloud storage that ensures the physical security of their data centers; employs strong authentication and authorization controls for all cloud compute, storage and networking infrastructure; and encrypts files using AES256-bit at rest and in transit to safeguard confidentiality. All data stored in the cloud should be encrypted by default to protect video at rest and all communications with to and from the cloud should be transmitted using HTTPS to protect data in transit.

The Verkada attack shows that the surveillance industry, specifically VSaaS, is vulnerable to hackers. With the increasing amount of sensitive video being generated, it's incredibly important that your cloud provider implement effective security measures to prevent these breaches. The best defense in deterring hackers or malicious intent is encrypted, uneditable, undeletable, immutable video provided by your cloud storage provider.

Move to the cloud at a pace that is right for you

The best first steps for the cloud journey

The growing importance of surveillance, higher resolution, and longer retention periods are the reasons why storage is taking a larger share of shrinking budgets. With the right video storage strategy, you can manage your infrastructure more efficiently, and stretch your budget dollars even further.

On-site storage has improved in both capacity and performance. Even their upfront acquisition costs continue to decline. However, this initial capital expense (CAPEX) represents only a portion of your total cost of ownership (TCO). The majority of expense comes after the initial purchase, in the form of hidden hard and soft costs. Scaling capacity means more boxes, more electricity for power and cooling, and less space in your facility.

As surveillance data ages, it becomes less and less likely that you'll need to access it. Up to 90% of your on-premises storage capacity can be this older video that could be off-loaded to lower-cost cloud storage—thereby freeing up your primary storage for the latest video files. You don't have to delete those older video files, which you might have had to do in the past without the unlimited scale of cloud storage, but it also doesn't have to be kept in the most expensive tier of storage.

Every gigabyte of video you clear from your primary storage translates into real-life savings because you are delaying the need to purchase additional on-site storage devices.

This is exactly why making storage the initial step to incorporating cloud services makes the most sense. It can save you significant money and well as reduce the burden of infrastructure management.

Storing video is easier than most people think. It just takes a few mouse clicks to configure cloud storage versus what used to take weeks or months in your on-site data center.

Eight benefits of hybrid-cloud architectures for video surveillance

- Investment protection of current mode of operation
- Open ecosystem to build best of breed solution
- Reduces on-site platforms to manage
- Scale devices and video quality with little impact
- Stream video files to the cloud during off hours, leaving network connections free during business hours
- Replicate locally stored video to the cloud for additional protection
- Continuous recording and access if the connection to the cloud is not available
- Access to video files from multiple geographic locations if needed

Conclusion: Use of hybrid cloud for video surveillance is on the rise

Like any other major technology project, using cloud services as part of the surveillance architecture needs a solid business case, one that takes into account all the likely costs and benefits, before an organization can decide whether it's the correct move.

With a hybrid approach to video surveillance storage, you can get the best of both on-site infrastructure and public clouds. By combining both, you can mix and match where you store your data to best suit your needs.

Hybrid cloud lets you leverage your existing on-site infrastructure while preventing the need to replace or extend that infrastructure with additional hardware as storage capacity runs out.

We are in the very early days of the cloud journey for surveillance use cases. Organizations can learn from the experience of others, especially corporate IT teams, where the pitfalls and obstacles to cloud adoption will be. All indications are that for medium and large size deployments, a hybrid-cloud architecture provides the best starting point.

Tips to keep in mind

Here are some tips to keep in mind when considering the cloud for surveillance video.

First, it's important to know if you're going to be charged to access your files or if there are micro charges for actions like API requests, data retrieval, and egress.

Second, make sure that your agreement isn't vendor exclusive. This could cause vendor lock-in and force you to use services that might have better alternatives.

Third, look for a pricing model that allows you to buy storage up front for a specific term at a fixed rate.

Consider storage providers that work in an open ecosystem with other surveillance technology solutions so you can easily move workloads.

Stone Security

Stone Security was founded in 2006 by law-enforcement and IT professionals with a goal to become the most trusted and sought-after security integrator in America. That ambitious vision still drives everything we do today. Although based in the Rocky Mountains, Stone Security does work all over the world. Several of our key clients have a global footprint and require the same quality installation and support regardless of location.

www.stonesecurity.net

Tiger Technology

Tiger Technology has been developing software and designing high-performance, secure, data management solutions for companies in Enterprise IT, Surveillance, Media and Entertainment, and SMB/SME markets since 2004. It was identified by the Endeavor group as one of the foremost cloud technology providers on the market today.

Customers are using Tiger solutions in over 120 countries. Tiger's software portfolio consists of high-speed NAS/SAN file system sharing, virtual volume set and virtual project workspace management in addition to an industry leading software-only cloud connector. Tiger Technology enables organizations of any size and scale to manage their digital assets on-premises, public cloud, or in a hybrid model.

www.tiger-technology.com

About Wasabi

Wasabi provides simple, predictable and affordable hot cloud storage for businesses all over the world. It enables organizations to store and instantly access an infinite amount of data at 1/5th the price of the competition with no complex tiers or unpredictable egress fees. Trusted by tens of thousands of customers worldwide, Wasabi has been recognized as one of technology's fastest-growing and most visionary companies. Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi is a privately held company based in Boston.

Tel 1-844-WASABI-1
Email info@wasabi.com

www.wasabi.com