

Hybrid Cloud Surveillance Solutions

Superior scalability and flexibility for enterprise level applications



What is a 'Hybrid Cloud' solution?

The definition can be confusing as subtle differences exist depending on context. In purely IT terms, the phrase Hybrid Cloud is primarily used to describe a solution that combines both private cloud (enterprise owned and managed) and public cloud environments (run by a third-party organization offering cloud computing services).

In a surveillance setting however, the phrase is more commonly used to describe a solution which combines on-premises hardware utilization with cloud-based resources such as Blob (Binary Large Object) storage for mid to long term video requirements.

In both instances, an important commonality is the presence of a single plane of management that ensures compatibility between the two separate environments, facilitating seamless control of data regardless of its virtual or physical location.

In other words, a single environment where the user or operator should not need to know or care where the data or services they need are hosted. For the remainder of this Tech Note, we will be referring to Hybrid Cloud in a surveillance context.

My surveillance solution allows remote viewing over the internet, isn't this the same?

Not necessarily. While your solution may allow remote viewing or storage using an internet connection, it is likely that recording, processing and management of data (video, audio or other sensor-related data) occurs on hardware installed at your site.

With a true Hybrid Cloud surveillance solution, data can of course still be recorded, processed, managed and stored on site, but these actions can also be done directly or indirectly to the cloud. This opens up a much higher degree of flexibility, both in terms of storage and collaborative working.

What are the main advantages of using a Hybrid Cloud solution for surveillance?

Hybrid Cloud solutions offer improved system scalability and usage flexibility. Two important examples in this respect are:

- **Easily increase storage capacity**

Storage requirements evolve. Increasing camera counts, adoption of higher resolution cameras/new technology, changing regulatory demands for footage retention periods: an organization may have to increase their storage capabilities for any number of reasons.

This can be problematic for on-premises storage. In addition to the capital expenditure required to increase hardware capacity, implications for physical space and energy consumption also have to be considered. Hybrid Cloud solutions remove this headache, offering a far more flexible and cost-effective way to store and access data virtually, without losing the ability to store information on premises (for example an initial 48 hours' worth).

- **Remote viewing, collaborative working**

Hybrid Cloud surveillance solutions are ideally suited for enabling collaborative working. For example, incident lockers and digital evidence management capabilities held in the cloud offer a fast, secure and resilient mechanism for sharing critical data with external third parties such as police or other emergency responders.

The implications are just as strong for facilitating higher levels of internal communication and collaboration between individuals and teams. With authorized, authenticated users able to receive and send data via devices connected to the cloud, efficient security and operational management moves out of the control room and into the field.

Does a Hybrid Cloud solution offer new opportunities for video analytics?

Yes. For example, with cloud platforms such as Microsoft's Azure or Amazon's AWS, a whole world of new opportunities are presented for integrating cutting edge developments such as cognitive services for video and image analysis.

Does Synectics offer a Hybrid Cloud solution with Synergy?

Yes, we offer our Synergy command and control solution as a true Hybrid Cloud option which utilizes Microsoft's Azure cloud infrastructure. With it, customers can span their surveillance and operational management system (primary/redundant Synergy servers, incident lockers, NVRs, specific integrations etc.) across on-premises and the cloud in any way they choose. All through our 'single plane of management' – the Synergy Client.

Data can be written directly to Azure's Blob storage or automatically migrated from on premises Synectics' PSNs after a user-defined period, according to needs/preferences. Wherever it is stored, Synergy knows where to look and how to retrieve it for instant access without the user having to worry about its location.

Are there any potential disadvantages of using a Hybrid Cloud surveillance solution?

Because advanced Hybrid Cloud surveillance solutions offer the 'best of both worlds' they overcome many of the challenges associated with a solution that is either/or. Here are three important examples:

- **Network outage**

The level of resilience that can be built into networks these days is massive, making a complete outage highly unlikely. In theory, however, if all data is being directly recorded to, stored in and accessed from the cloud, a network outage could mean losing access to that information for the period of the outage.

Advanced options, like our Synergy Hybrid Cloud solution, mitigate this risk by giving users the option to record an initial period of footage – perhaps 24 or 48 hours – on-premises as back up.

- **Storage decisions**

While infinitely scalable, cloud-based solutions (full or hybrid) often work on a pay as you go basis linked to access. For example, the highest level may offer instant and unlimited access. But this will also incur a high cost and for users that may only need to access cloud-based footage part of the time – for instance to collaborate on incident/evidence review – this 'always on' facility may be an overly expensive option. A mid-level option may offer the same degree of data access but at a lower upfront cost because in this



case, the user pays each time footage is accessed. Finally, a lower 'archive' level may have minimal up-front costs, again employing a pay-to-access mechanism, but also have restrictions on how fast data can be accessed, potentially delaying access to critical information.

This can present a challenge for users with changeable/unpredictable storage and access needs. Our Synergy Hybrid Cloud solution overcomes this by allowing fluid migration of data between on-premises storage and between the different cloud storage levels, either on an automated basis (for example based on data source/type/retention period reached) or manually driven by a Synergy user.

- **Frame rate**

While many cloud-based VSaaS solutions (Full Cloud or Hybrid) offer greater flexibility, it can come at the expense of frame rate in order to minimize bandwidth utilization – around five frames per second is common. Depending on the specific surveillance requirements, this may be fine but for mission critical evidence review or live incident monitoring, this could be insufficient. We have developed the Synergy Hybrid Cloud solution to ensure that even at 4K resolution, a minimum of 30 frames per second is guaranteed.

Is my data as protected in a Hybrid Cloud environment?

Yes. Data sovereignty and protection is a concern often raised when talking about either Full Cloud or Hybrid Cloud surveillance solutions; 'where is my data going?' and 'who exactly can access it?' are understandable questions to ask. But the reality is that cloud-based solutions offer an extremely high

level of protection often with military grade encryption and multi-factor authentication.

To illustrate, here are three important ways data sovereignty and protection is guaranteed with our Synergy Hybrid Cloud solution (in addition to data protection and user authentication protocols already present in Synergy):

- **Control over data center location**

All our users have the ability to choose the country in which their cloud-based data is stored, in other words the location of the data center.

- **Protection of communication via security certification**

Every device connected to the Synergy cloud environment in Microsoft Azure has a unique security certification. This certification cannot be replicated and without it, a device cannot connect. Similarly, an active directory of user authentications provides additional layers of protection.

- **Data encryption**

In addition to the data encryption which takes place natively within Synergy, all communication between a Synergy Client and the cloud is also encrypted.

Are there any important network infrastructure requirements to consider?

Sufficient network bandwidth and delivery quality are essential for ensuring data is transferred to the cloud reliably. However, the increase in affordable available bandwidth from Internet Service Providers, plus a growing number of opportunities for redundant connections, means this is no longer the issue it once was.

Synectics

sales@synecticsglobal.com
synecticsglobal.com

Specifications subject to change. E & OE.

Literature Reference: HC-TN/0821/A4 Iss 1
Copyright © Synectic Systems Group Limited 2021. All Rights Reserved.