White Paper

Video surveillance as a service (VSaaS)

What aspects do you need to assess to decide if the cloud is the best fit for your video surveillance project?

Although the possibility of hosting data in virtualized and remote storage spaces was already conceived in the 1960s, the practical application of this new usage model, especially in the field of video surveillance, and its commercialization at the professional level is relatively recent.

New technologies have enabled the possibility of creating an environment where video and applications can be stored without the obligation of owning an infrastructure to maintain it.

The cloud is currently one of the trends that will most affect the electronic security sector due to connectivity and cost reduction by minimizing investment in hardware equipment and system maintenance. But is the cloud the most suitable option for storing images from any video surveillance system?

In the following article we tell you the aspects to take into account to decide if a CCTV system in the cloud is the most suitable for your installation.

Internet connection

Logically, network infrastructure and connectivity are key to guarantee bandwidth with Quality of Service (QoS) and high image availability to avoid losing the video signal in the event of any Internet connection outage.

It is of little use for the provider to offer all the necessary redundancies to guarantee the service if we transfer this element of failure to the availability of our Internet connection. A drop in our connection would result in a loss of all recordings for the duration of the drop.

In addition to the bandwidth we will have to assess whether the video surveillance system incorporates video analytics as they require more computational processing at a centralized site.

White Paper

Risk analysis

A little over a month ago, a fire destroyed some servers of the French company OVHcloud, the largest European cloud service provider.

Its customers, including the French government which has national data open to the public with OVHcloud, had to activate their disaster recovery plans.

The causes of loss of connectivity can be multiple and uncontrollable and in any case a risk analysis will have to be performed to know how critical the loss of images is for our customers and to establish an image recovery plan.

Storage

Knowing what we want to transmit and for how many days we want to keep the recordings will be a priority for sizing storage needs. In addition, we must take into account the need for BackUp or Redundancy.

The available bandwidth must be adapted to our recording needs, i.e. the number of cameras in the installation and the resolution and framerate with which we intend to record.

Assuming that the cameras offer the most advanced compression standard protocol currently available (H.265), we can be talking about a total of 2Mbps for a 2 Megapixel camera at 25 frames per second.

If we have an average of 10 cameras in the installation, we will need a total of 20Mbps guaranteed upload per site, only for the CCTV. If for the same site, we consider standard resolution analog cameras, connected by encoder (H.265) and recording at 4CIF at 10 frames per second, the bitrate per camera would be about 700Kbps on average, which would mean a total upload bandwidth of 7Mbps.

Therefore, in a market with a clear tendency to offer more and more resolution in its cameras, it is also important to evaluate the bandwidth requirements to validate its viability in each geographic region, as well as the cost involved in such a connection.

Cost calculation

While it is true that the cloud eliminates the cost of hardware storage equipment, it is necessary to take into account certain hidden costs that are not included in the monthly subscription fee and that are difficult to quantify: the cost associated with the loss of images, penalties for non-compliance with current legislation, the wrong sizing of the necessary storage, and the cost of downloading information that in the case of video surveillance, we are talking about high definition images and videos that involve many GB/TB of data download, which can increase the cost exponentially.

Existing CCTV infrastructure.

If the installation currently has an analog CCTV system, in order to enjoy the advantages that the cloud can offer, it will be necessary to consider whether to migrate to IP technology or invest in encoders that transmit the signals from the current analog cameras.

White Paper

Data protection and cybersecurity.

Although it is true that, historically, there have been successful attacks on large technology companies, these types of services are usually very technologically prepared to repel cyber-attacks.

What is a reality is that the user stores the data remotely and no longer has direct control over it, with the risk that this entails, since video is very sensitive and confidential information.

At all times the information must travel securely and encrypted, for which we will need to have cybersecurity measures to protect our clients' data (images): Firewall, IDS, etc.

In the event that we value opting for storage in a public cloud (Amazon, Microsoft, etc.), we must be aware that the client's data is being managed by a third party and therefore there may be legal problems associated with the ownership of the images and there is a dependence on uncontrollable factors: connection, storage, security of the third party, etc.

Specifically, the IaaS (Infrastructure as a Service) provider must take the necessary measures to promote the correct application of the GDPR (General Data Protection Regulation) as they are responsible for storing the images we record.

In early March 2021, a group of hackers accessed images from more than 150,000 video surveillance cameras from customers of Verkada, a company that sells security cameras that customers can access and manage over the network.

The cyberattack exposed the security of hospitals, prisons, and even the factories of Tesla, the automaker. This would not have happened on a customer's local private network with a well-secured VPN.

Integration

In the case of having other intrusion systems, access, etc., it will be necessary to consider taking them to the cloud so that they can interact with the video systems, not to mention the problems of integration with other security elements that can be found physically in the installation.

The cloud undoubtedly offers numerous advantages in terms of connectivity and costs, but it will be necessary to know the needs of each installation to find out if Cloud Computing is the most suitable solution for the storage of your images.