5 things to consider before moving your surveillance to cloud-based video storage

Published on 19 Jan 2016

Determining how the cloud can best support your business depends on five factors: Bandwidth, storage, cost, security and accessibility

Until about a decade ago, most enterprises used their video surveillance systems primarily to view live video or review security incidents after the fact. Today, many are taking advantage of intelligent video solutions to reduce losses from theft and fraud, monitor and improve customer service, track commercial conversion rates and performance trends, and identify opportunities to strengthen their marketing, operations, compliance and sales strategies.

At the same time, enterprises across all sectors are leveraging technology solutions such as the cloud to reduce IT costs, streamline application management, and make their infrastructure more flexible and scalable. So it’s no surprise that these same companies are now turning their attention to emerging cloud applications for video surveillance.

Yet video surveillance solutions have some unique requirements that set them apart from other types of enterprise cloud applications. Video — especially high-definition video — demands much more bandwidth and storage than the consumer-oriented cloud services you may use at home.
Security and privacy have to be considered, too, as regulations and corporate policies may all impose restrictions on the transport and storage of video footage. And the anticipated return on investment, of course, is always a consideration when evaluating any technology solution.

Ultimately, determining where and how the cloud can best support your business depends on a set of five primary requirements: bandwidth, storage, cost, security and accessibility.

Businesses should assess the advantages & disadvantages of the cloud solution compared to the existing VMS with respect to bandwidth, storage, cost, security & accessibility

1. It all begins with bandwidth

The total bandwidth required for a video stream varies depending on the number of frames or images being captured per second, as well as the quality of the images being captured. Given that most enterprises are now replacing some (or even all) of their older analogue cameras with new megapixel IP cameras, bandwidth becomes an even more important factor to examine.

Many enterprises today, surprisingly, still do not have the bandwidth capacity to upload video captured by multiple IP cameras to the cloud. Even if they employ buffering, which can limit video streaming until a time when more bandwidth is available (such as after business hours), few
organisations can access the required upload speeds consistently at all locations, especially those operating hundreds or thousands of sites.

And while bandwidth speeds and accessibility will continue to improve, and therefore ease the barrier toward efficient video uploading to the cloud, the trend toward multi-megapixel IP cameras may counteract that advantage.

Even the organisations that do enjoy high-speed, high-capacity upload connections across all of their locations may not be in a position to dedicate all (or even a sizeable portion) of their network resources to their video surveillance systems. In fact, it’s quite common for banks, retailers and other enterprises to restrict or ‘throttle’ the network capacity allotted to video to just 100–200 kb/s of their total bandwidth to ensure their corporate network has the capacity needed to transmit business-critical data.

Service provider caps on broadband services represent another constraint to sending and storing video in the cloud. Again, even locations with sufficient upload and download speeds may have limits on how much data they can push through the network. Exceeding the limit can incur additional — and often prohibitively high — costs.
2. Making sense of storage

Before moving video surveillance to the cloud, enterprises also need to consider that the majority of collected video is never used — at least by organisations that are not yet leveraging their video’s broader business analysis capabilities — because only specific events will trigger follow-up action. It is therefore important to determine when it makes sense to transmit video data for storage over potentially expensive network links.

Assuming that a company has been able to overcome the bandwidth barrier, the cloud could provide ‘unlimited’ storage, the cost of which will presumably continue to decrease as technology improves. Even so, companies should determine how long they need to archive their video and how much redundancy they require, as both factors may add to the total cost of their cloud storage solution.

3. Cybersecurity risks and vulnerabilities
With video surveillance systems increasingly connected to the Internet, it is critical that they receive the same level of attention to cybersecurity risk and vulnerabilities as traditional IT systems such as servers and workstations. Given the legal, financial and reputational risks associated with data breaches and leaked video, enterprises are intensely concerned about ensuring the integrity and security of their video networks.

Port forwarding, firewalls, network topology and video encryption can all have a significant impact on the security and protection of a cloud-based video surveillance system, requiring a greater degree of expertise and effort in these areas on the part of an organisation’s in-house IT support team.

At the same time, some companies have internal policies that strictly prohibit video data from leaving the corporate network or having it stored on a third-party server (even one run by a trusted and reputable provider); others prefer not to take the risk whether or not their formal policies preclude using the public cloud.

Even if video data is stored on a local server rather than in the cloud, security and privacy remain important concerns, with data protection and user authentication being two key considerations.
Port forwarding, firewalls, network topology & video encryption can all have an impact on the security & protection of a cloud-based video surveillance system.

4. Local network access vs. third-party networks

Relying on a third-party network to upload or download video means any outage could cut your organisation off from its video assets. Uploads may fail, data may be lost and information may be unavailable until the service comes back online.

Consider how frustrating it would be to sit in a security control room knowing that all your cameras are recording, but not being able to view what they’re capturing because the external network is down. In the very worst case, a network outage could cause data loss. Packets that can’t leave the location might be overwritten or discarded, leaving no video record at all. This would be especially unfortunate if a robbery or violent incident was not recorded as a result.

When video is stored on premises, there’s always the comfort of having local access and control. Most enterprise-class servers and network video recorders (NVRs), for example, include battery backups to ensure video recording continues in the event of a temporary network outage.

5. Assessing cloud service provider

Cloud-based video surveillance storage and management is an emerging approach with considerable potential. However, until the substantial bandwidth challenge can be overcome, it won’t offer a cost-effective alternative to today’s video surveillance solutions for most mid- and large-
sized enterprises with multiple locations and more demanding video requirements.

As with most network technologies, the point of feasibility will be reached over time as new solutions emerge and build on previous technical capabilities. In the longer term, advances in video compression and faster, more affordable bandwidth services will help make cloud-based storage solutions a more viable option for many larger, multi-site enterprises.

When exploring the opportunities associated with the cloud, it is important to move beyond the hype and take the time to carefully consider the implications a cloud-based video solution may have on your business. This should include preparing an appropriate set of questions to ask of any potential cloud service provider so you can accurately assess the advantages and disadvantages of the solution compared to your existing video management system, especially with respect to bandwidth, storage, cost, security and accessibility.

Author Profile

Dan Cremins
Clarifying misconceptions about video storage solutions

One key misconception is that solid-state drives (SSDs) are going to replace hard disk drives (HDDs). Like many areas of technology, the transition is gradual and influenced by factors such as cost, performance, and reliability.

How latest NVR technologies adapt to storage challenges and other deve...

NVRs make it easy to benefit from HD solutions and integrations to access control, alarm systems, intercoms and other technologies.

How to achieve high quality video with lowest bandwidth and storage needs...

A lower bitrate reduces bandwidth and storage requirements. High definition and megapixel cameras provide more detailed images.