Comparative Review of VSaaS and Local CCTV Recording and Management

By Nigel Stanley

MSc (Lond.) CEng MIET MBCS MIEEE

Practice Director – Cyber Security

OpenSky UK

7th April 2015

Contents

Executive Summary

Every year, our society grows more reliant on the use of CCTV: to prevent crime, monitor remote sites, or even care for the elderly. Over the years, CCTV systems have evolved, from the most basic TV monitors, through VHS recordings, to IP-enabled cameras producing high-quality digital images.

The final technological leap in visual surveillance has been the move to hosting images in the cloud. Long considered a cumbersome necessity, inefficient CCTV systems are changing. Cloud-based alternatives – dubbed Video Surveillance as a Service (VSaaS) – are now transforming the way we use CCTV.

- Cloud technology is widening the scope of CCTV applications. No longer the preserve of criminal investigators, remote monitoring allows organisations to use CCTV to safeguard their assets and families to ensure the safety of their loved ones.

- Impractical and time-consuming data retrieval processes are simplified by centralised cloud storage and a user-friendly browser interface.

- Traditional security and compliance concerns are resolved by the encryption of data at a local level, and its transmission, off site, into the cloud. In this way, data is removed from the risk of theft or physical damage - deliberate or otherwise.

- Secure storage in the cloud preserves the confidentiality, integrity and availability of data.

- This enables organisations to easily comply with Data Protection legislation.

- It also simplifies and speeds up any necessary investigations, reducing the need for site visits.

Until recently, surveillance technologies have been a burdensome essential, costing organisations valuable time and money. Fortunately, with the right planning and processes in place, it is easy to implement secure and successful VSaaS systems, reducing risk for businesses and individuals.

Introduction

Following significant government investment in the 1990s, closed circuit television (CCTV) use in the UK exploded. Now seen almost everywhere in the public and the private domain, CCTV cameras can play a legitimate part in the reduction of crime and the identification and subsequent apprehension of offenders.

Furthermore, new applications for CCTV continue to emerge.

The growing number of care homes providing for an ageing population has coincided with increasing concern amongst relatives as to quality of care. The judicious use of CCTV in this environment can improve standards whilst addressing privacy issues, and provide a clear audit trail, should any problems arise.

Brands are extremely valuable to companies of all sizes; often, protecting those brands remotely can prove difficult. Where corporate infrastructure or products and service outlets are scattered across multiple locations, companies have traditionally needed to deploy teams of personnel to inspect and maintain them. Now, CCTV can monitor these assets, goods or services, providing immediate assurance of their integrity.

The Evolution of CCTV

First generation CCTV employed analogue cameras connected to a black and white TV monitor, requiring the full attention of security teams based in custom-built monitoring centres. The advent of cheaper video recording devices reduced the need for constant vigilance, making VHS tape the recording medium of choice.

The catalyst for the initial growth in CCTV recording was the introduction of video multiplexers that allowed multiple cameras to record to a single time-lapse video recorder using VHS tapes. A picture from each camera would be recorded every few seconds.

Image quality was often poor and recording capacity limited, due to the available size of the videotape. Frequent re-use of video tapes lead to a gradual degradation of image quality, in many cases rendering any evidence useless.

The transition to local digital recording media - usually in the form of a DVR (Digital Video Recorder) with hard disc local storage - saw an improvement in the quality of image recording and processing. However, with no parallel improvement in camera technology, poor quality images remained the norm.

Since then, vastly improved systems have been deployed to take advantage of enhanced computer-controlled storage and processing of new or upgraded digital cameras to deliver high quality images.

However, the fundamental weakness with all of these installations is the need to process and store image data locally.

Local storage is costly to purchase and can hugely increase the time, effort and resources required to access recordings if needed. After an incident, the police or property owner must visit the relevant site, often in conjunction with a specialist CCTV company. At this point, it is common to encounter technical issues - such as media incompatibility, or even failed access due to forgotten passwords.

Even when the data has been recovered, there is no guarantee that it will display the correct time stamps, and the integrity of evidence is reliant on the subsequent chain of custody. In many cases, there are no technical controls to preserve the data – just a plastic evidence bag with a unique serial number.

The good news is that there is now an alternative. Following the evolution of cloud computing into a commoditised, easily-accessible platform, cloud-based CCTV is gaining a strong foothold. Dubbed 'Video Surveillance as a Service' (VSaaS), cloud solutions are transforming the world of CCTV.

Introducing the Cloud

The concept of cloud computing goes back over 60 years to when mainframe computers were first enabled to share their computing time to third parties, such as universities and research establishments.

Today's cloud computing enables anyone with access to the Internet to benefit from the vast storage and computing power from the recognised experts such as Amazon, Microsoft and IBM.

Generally, the key drivers for the adoption of cloud-based computing are its lower running costs, cross-platform flexibility, and the ease with which additional storage can be brought on line.

Quite simply, building and maintaining a server infrastructure is expensive, and for many business, not a priority. The ability to outsource this to a third party who specialises in the tools, technologies and infrastructure of computer servers is very compelling.

However, cloud-based computing does raise questions of security.

Security

In the past, organisations would create and maintain their own physical computer servers, locked away in a private server room under their strict control. With cloud computing data is usually sent to an amorphous mass of servers (hence the term 'cloud' computing) whose location will normally be unknown. In many instances, data can reside in an overseas jurisdiction, out of local control.

As such, there remain certain risk and security related questions which must be addressed before customers feel comfortable adopting a cloud-based system. In reality,

many of these issues have been addressed over the past few years, and many customers will see a cloud-based system as more secure, resilient and reliable than anything they could build or manage themselves.

For those still in doubt, a private or hybrid cloud solution can often deliver many of the benefits of cloud computing but with greater customer control over the server infrastructure.

The move to the cloud is already impacting the delivery of public services, even from well-established institutional systems. For example, the UK government is a strong advocate of cloud-based computing; government departments can purchase services in a cloud–hosted, virtual marketplace known as the G-Cloud.

With a suitable risk assessment, then, cloud computing could be a valuable pillar of many organisations' IT strategy.

Practical benefits of cloud-based CCTV

It seems only natural that CCTV image data would be a strong candidate for storage in the cloud. Locally stored data is subject to the usual limitations of local storage media – both VHS and DVR have a finite storage capacity. Local hard discs eventually fill up. By contrast, a contract to store visual data for 30 days in the cloud can be flexible as to the physical volume of data stored –so you won't run out of space. The ubiquitous nature of the Internet - accessible from almost anywhere - makes it relatively straightforward to connect cameras via Ethernet, wireless, 3G or even satellite. Cloud-based CCTV also simplifies access to CCTV images, requiring only a web browser and the appropriate authorization to login and view the data. Because all the components involved are connected to the internet, clock timing can be constantly verified and synchronised to ensure that all recordings are tagged appropriately.

Cloud CCTV for Investigations

Following an incident, one of the first questions many investigators ask these days is if there are any helpful CCTV images. From domestic burglaries through to armed robberies, street assaults and antisocial behaviour, access to CCTV can be hugely valuable for the investigation team.

Then comes the problem: how to seize the evidence? For an ongoing investigation, accessing and exhibiting CCTV evidence is time consuming and slow. In a real-time incident, such delays can be life threatening.

So what are the traditional options?

The first is to ask the CCTV controller for the DVD or VHS tape for the relevant time period and date. Investigators must ascertain whether the system has been configured correctly, with accurate time stamp settings – otherwise, hours of recordings may need

to be viewed. Assuming that the correct media can be found and that it has not been overwritten in a media-recycling process (for example after a typical 7-day or 30-day cycle), the investigator can ask for the media. Without police or court powers, forcing evidential handover is almost impossible - so if a polite request is refused or ignored, there may be a problem.

It is possible to produce a copy of the evidence, but this can call into question its forensic integrity. In digital forensics, such doubts are overcome by seizing the original media and reproducing it in the form of working copies. These copies are forensically sound, bit-by-bit replications of the original – a process that can be proved using cryptographic hashes.

Of course, all this assumes that the investigator is able to copy the media using the technology available onsite and in their own tool kit – not always an easy thing to do. For this reason, seizing the original media is often considered the lesser evil.

Some companies that provide public services, such as transportation and venue management, can be inundated with requests for CCTV evidence. In many cases, this necessitates employing full time staff just to do the job.

Once seized by an investigator, the VHS or DVD evidence will need to be properly stored and exhibited, and only returned to the owner once the case has been resolved. Although recording equipment is not necessarily expensive, even the most happily cooperative CCTV operator tends to lose patience if multiple requests are made on a regular basis, and then sometimes lost in the system or otherwise damaged.

Moreover, this works on the assumption that the CCTV media remains intact and on site following an incident. In reality, most criminals these days are aware of the use of CCTV. The DVD or VHS recorder will often be deliberately disabled and the media destroyed during the incident.

Practical issues of managing DVR equipment

The practical problems with managing CCTV via hardware on premises have already been addressed briefly. Without dedicated staff to manage and maintain the equipment, it will very quickly fall into disrepair. In the worst case, CCTV equipment will be tucked away in a store room, at risk of becoming unplugged or otherwise neglected. After all, few businesses can afford to waste resources on the upkeep of their surveillance systems.

Even the best maintained CCTV setups see mistakes made, as media gets accidentally overwritten or time and date stamps become corrupted - frustrating any subsequent investigation.

In the past, older CCTV systems that relied on coaxial connections and hardwiring for cameras and control consoles were often difficult to upgrade and alter. Running

additional cabling for new cameras or installing additional monitoring stations was often difficult and expensive. The move to IP-enabled cameras addressed a number of these issues, but it is only with a VSaaS system that full use can be made of the Internet and the cloud.

VSaaS enable multiple cameras and multiple sites to be aggregated and controlled from a single web browser interface (or even smartphone), simplifying use and securing access.

Locally hosted CCTV system security and VSaaS

As previously discussed, the perceived lack of security is usually the first objection to any system that makes use of cloud-based servers.

By nature, CCTV images often contain sensitive data that may be subject to some form of investigation. If these images are tampered with, destroyed or otherwise compromised, the evidence will be tarnished – or worse, lost altogether. For many, the idea of tangible CCTV hardware with a set of recordings offers a sense of comfort that is missed when dealing with remotely hosted images. Data protection issues also come to mind - especially if data is stored out of a local jurisdiction, with insecure access restrictions.

Adapting to a VSaaS mostly requires a change in attitude; concerns regarding data protection and security can be easily addressed. Image data must always be managed according to the standard information security triad of confidentiality, integrity and availability.

Confidentiality – ensuring only the right people and processes have access to the video data at the right time.

Local CCTV systems are often physically insecure and access to recorded media can be unprotected. In many instances there are few controls on who can access the room in which a local CCTV system is stored, so it is difficult to produce an accurate audit trail. In addition, the recordings may not be encrypted or otherwise security protected by default.

With VSaaS systems, access can be restricted using security controls such as a login name and a strong password. Data encryption can be used to ensure image data remains confidential as it is transferred from a visual network adapter (VNA) to the cloud storage system. Once on the servers, the data remains encrypted, only available to those with the appropriate decryption keys.

Integrity - making sure that the data remains in its original form and has not been tampered with.

Standard media such as a DVD recording could be tampered with and images re-recorded with little in the way of automatic checks to demonstrate the integrity of the

original data. In a cloud-based system, integrity is normally enforced using a cryptographic primitive called a hash. This uses a function that processes the video data in such a way that any attempt to alter or change it will be obvious.

Availability – ensuring that the system and data are available to legitimate users at all times.

Locally managed CCTV systems are vulnerable to power outages and hardware failures, and can be accidentally or deliberately switched off. Recorded media can be lost, stolen or destroyed (in a fire, for example), severely hampering evidence recovery.

By contrast, cloud-based systems are engineered to provide a robust service level agreement so that annual uptime is guaranteed. 99.99+% availability equates to only 52 minutes downtime per year; if the internet goes down, then advanced systems will automatically recourse to a local SD micro card, enabling continued recording. Images are then uploaded when the connection is re-established.

Managing image size and bandwidth

Many computer networks have been designed to deal with relatively low volumes of data such as email and basic file transfers. This is especially the case in small and medium sized businesses that may be using shared or domestic type broadband services. Larger businesses will often have a more complex networking environment with better access to the Internet; nevertheless, bandwidth will often be at a premium.

Burdening such networks with CCTV image traffic can have a significant impact on performance, as live video streaming can be costly in terms of bandwidth. Most VSaaS systems will smartly manage their bandwidth consumption, throttling it as appropriate. Image capture frame rates can also be tailored to suit network capacity.

Regulatory and compliance issues

In the UK, CCTV system operators are subject to the Data Protection Act 1998. The Information Commissioner has produced a data protection code of practice for the use of CCTV and similar systems; operators who stick to these guidelines should have no problems. Operators of cloud-based CCTV systems are no exception, and will need to ensure that their obligations under the Act are still met.

As it is hosted remotely, a cloud-based system can be accessed by any user with the right credentials and a web browser – great for usability, but something that introduces additional risk. So, it's important that cloud-based CCTV accounts are managed according to a security policy, and that starters/leavers/movers are given the correct access rights. More importantly, accounts must be deleted when a user leaves or no longer requires CCTV access.

It is easy to fall into the trap of keeping images for longer in a cloud-based system than in comparable physical systems. However, The Data Protection Act and the Surveillance Camera Commissioner stipulate that images are only stored for as long as can be justified.

Destroying or overwriting locally held media is easy, but cloud-based data destruction needs to be evidenced differently - normally by maintaining accurate online activity logs and records of file creation, access and deletion.

Managing physical evidence can be a challenge; for many years, it has been accepted practice to present the court with a sealed evidence bag, uniquely numbered and fully recorded with a provable chain of custody.

Translating this rigour to the world of cloud-based CCTV images can be technically challenging. The usual mechanism is to apply a cryptographic hash function, which takes a known input (this is the original CCTV data, called the message), and processes it to produce an output value called the message digest. The message digest will be unique for any set of CCTV data, and as such it will be unfeasible to create any other CCTV data with the same value.

This hash function can prove whether CCTV images have been altered or changed, as any subsequent message digest will have a different value.

Conclusion

In recent years, we have seen CCTV adopted across society to help care for loved ones, safeguard assets, and manage business risk. Meanwhile, law enforcement and the courts have also become increasingly reliant on the evidence gathered from such surveillance systems.

Technologies such as VHS video tapes and DVR recorders have already made conventional CCTV systems a little easier to use. Until recently, though, a lack of innovation meant that CCTV was falling behind in the technological race to secure assets, people and processes.

The arrival of VSaaS now presents a tremendous opportunity for dated CCTV systems to engage with the 21st century – embracing flexible cloud technologies to improve the manageability, security and reliability of this crucial visual surveillance tool.

	Locally Hosted CCTV	VSaaS Cloud-based CCTV
Image Data Security - Confidentiality	Some systems may have password controlled access. Image recordings are stored locally and are subject to theft or destruction	System can be secured using a combination of user logins and passwords. Image recordings are stored remotely in the cloud
Image Data Security - Integrity	Local storage media may be easier to access and tamper with	Use of hash technology will ensure that any image tampering can be identified
Image Data Security - Availability	Local storage is finite. Images may be accidentally erased. Image quality can suffer following multiple overwrites of VHS recordings	Cloud-based systems can achieve high availability (99.99%). If a connection is dropped local edge recording can still be supported
System Management	Systems may require direct local access and attendance to recording equipment	Systems can be managed by anyone with access to the web

Appendix 1 – About the author

Nigel Stanley is a specialist in information (cyber) security and business risk, with over 25 years' experience in the IT industry. He is a well-recognised thought leader and expert capable of delivering complex cyber security projects across small, medium and large scale enterprises.

Nigel has in-depth knowledge of cyber security, information security, business risk, data breach incident response, digital forensics, business continuity, cyber warfare, cyber terrorism, mobile device security, BYOD, smartphone security, application development, software development, systems engineering, SCADA and industrial control systems.

He has significant radio and electronic engineering experience and regularly advises the law enforcement community on technical issues relating to criminal investigations.

Nigel has written three books on database and development technologies and is a regular conference speaker. He has presented papers at InfoSec, IFSEC and IPEXPO as well as at numerous webinars and online events.

He is able to bring together his technical knowledge and his practical experience of cyber security and business to help clients benefit from information security.

Nigel is a Chartered Engineer and member of the Institution of Engineering and Technology (where he sits on the IET Cyber Security Steering Group), Institute of Electrical and Electronic Engineers and the British Computer Society.

He has an MSc in Information Security from Royal Holloway, University of London where he was awarded the Royal Holloway University Smart Card Centre Crisp Telecom Prize for his MSc research dissertation.

Appendix 2 - About OpenSky

OpenSky Corporation provides information technology expertise to help corporations optimise IT platforms, protect information assets and accelerate the adoption of strategic technologies. We specialise in transformational IT infrastructure, cyber security and compliance consulting.

We help enterprises with:

- Planning for IT optimisation initiatives.
- Shifting computing to virtual and cloud based infrastructures.
- Developing next generation applications and data centres requiring next generation security and application security.
- Managing and securing the proliferation of BYOD and mobile devices.
- Mitigating risk and compliance across the organisation.
- Developing highly functioning IT organisations while reducing costs.

OpenSky is distinguished by its combination of extensive technology expertise and deep industry experience. OpenSky specialises in Infrastructure; IT Risk Management and Security; Governance, Risk and Compliance; and Technical Business Consulting.

OpenSky has successfully delivered over 750 projects to Fortune 500 companies. Proven methodologies ensure a focused, consistent, project-based approach on every engagement. OpenSky maintains a business-centric perspective and believes that aligning premier technology partnerships with vendor-neutrality are critical in ensuring the best solutions for clients.

TÜV Rheinland, is OpenSky's parent company and a $2B global leader in independent testing, inspection, certification, and consulting services. OpenSky believes that a highly experienced and qualified IT consultancy plays a valuable part in the design, optimisation and security of IT and business.