VSaaS:

11 Reasons Why Video Surveillance is Moving to the Cloud

A Detailed Comparison of VSaaS vs. Internet-Connected Traditional Security Camera Systems

By Dean Drako, CEO of Eagle Eye Networks

VSaaS, or Video Surveillance as a Service, refers to hosted cloud-based video surveillance. The service typically includes video recording, storage, remote viewing, management alerts, cyber security and more. 93 percent of businesses have now adopted cloud solutions. Cloud technology advances and greater bandwidth availability are making VSaaS - also called cloud video surveillance – is increasingly attractive.

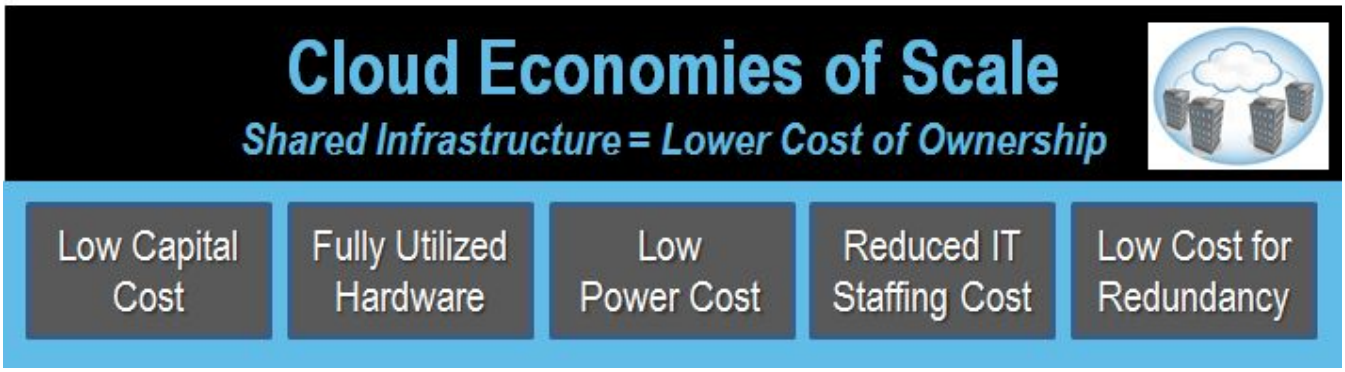
This white paper will clarify the fundamentals for a true cloud system, using guidelines set by the US Department of Commerce's National Institute of Standards and Technology.

It provides an 11 point comparison of key differences between "VSaaS" cloud-based video management system (VMS), and an internet-connected traditional DVR, NVR, or VMS. This checklist can help you assess which system type will best fit your company's and/or your customers' needs.

TABLE OF CONTENTS

1. CLOUD ADOPTION AND ECONOMIES OF SCALE

More than 9 in 10 business are currently using cloud technology, including email, phone, backup, applications, and increasingly, video surveillance. A survey of 930 respondents using cloud infrastructure showed that 88 percent achieved savings. 60 percent were able to reduce IT support, often redeploying IT personnel to other projects. Almost half (49 percent) were able to grow their business from cloud use. Cloud technology offers businesses substantial economies of scale. Let's take a look at the various cost savings, all contributing to lower total cost of ownership.



Lower upfront capital expenditures. A well-established cloud savings benefit is the reduced upfront capital costs, offering companies the opportunity to invest precious capital into other business areas, whether it is cash on hand or borrowed money.

Fully utilized hardware. Because multiple companies share server infrastructure, hardware is more fully utilized, and the cost for supporting workloads goes down

Lower power costs. Better hardware utilization means no idle servers. When you run your own data center, you will rarely fully-utilize your servers. Idle servers waste energy. So the better hardware utilization of the shared infrastructure also means more efficient power use, and the energy costs are lower.

Reduced IT Staffing Costs. The expenses associated with experienced IT personnel, including salary, benefits and other employment costs, is typically greater than the cost of hardware and software. The cloud provider's IT staff supports a shared infrastructure, so the total IT personnel cost is lower than if you did the work in-house. Thus you can reduce your own IT expenses, or redeploy employees to areas generating greater income.

Reliability & Redundancy. To achieve a highly redundant and reliable system, you must purchase additional

hardware to protect against failures. Having spare hardware lying idle is an expensive way to maximize uptime. Typical cloud systems have several data center locations.

2. FUNDAMENTAL ELEMENTS OF A "TRUE CLOUD" SYSTEM (VSAAS)

Cloud technology is still new enough to video surveillance that there is some confusion. A true cloud video surveillance system - or VSaaS - with its associated benefits, is very different from a traditional DVR, NVR, or video management software (VMS) solution connected to the internet for remote access or remote storage.

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has created The NIST Definition of Cloud Computing which can help clarify some of the differences. NIST defines a cloud system as having five "essential characteristics", as summarized below.

1. On-demand self-service. A user can automatically set and adjust capabilities without requiring human interaction with each service provider.

2. Broad network access. The capabilities are available over the network and accessed through standard mechanisms that promote use by thin or thick clients, such as mobile phones, tablets, laptops, and workstations.

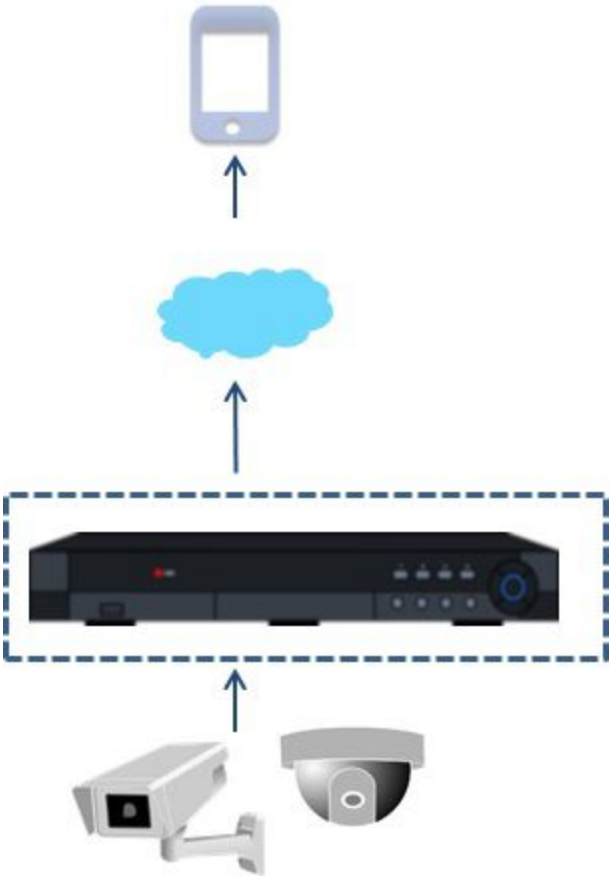
3. Resource pooling. The service provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and re-assigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth.

4. Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

5. Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency.

To deliver these five "true cloud" essential characteristics the compute resources are executed in a shared cloud infrastructure – it can be a public or a private cloud. Let's look at how this works for video surveillance systems

Internet-Connected Traditional DVR/NVR/VMS



With a traditional system, the video processing and management occurs on a computer installed at your site.

This video may be later accessed via an internet connection for viewing or archival storage.

Cloud-based VMS / VSaaS

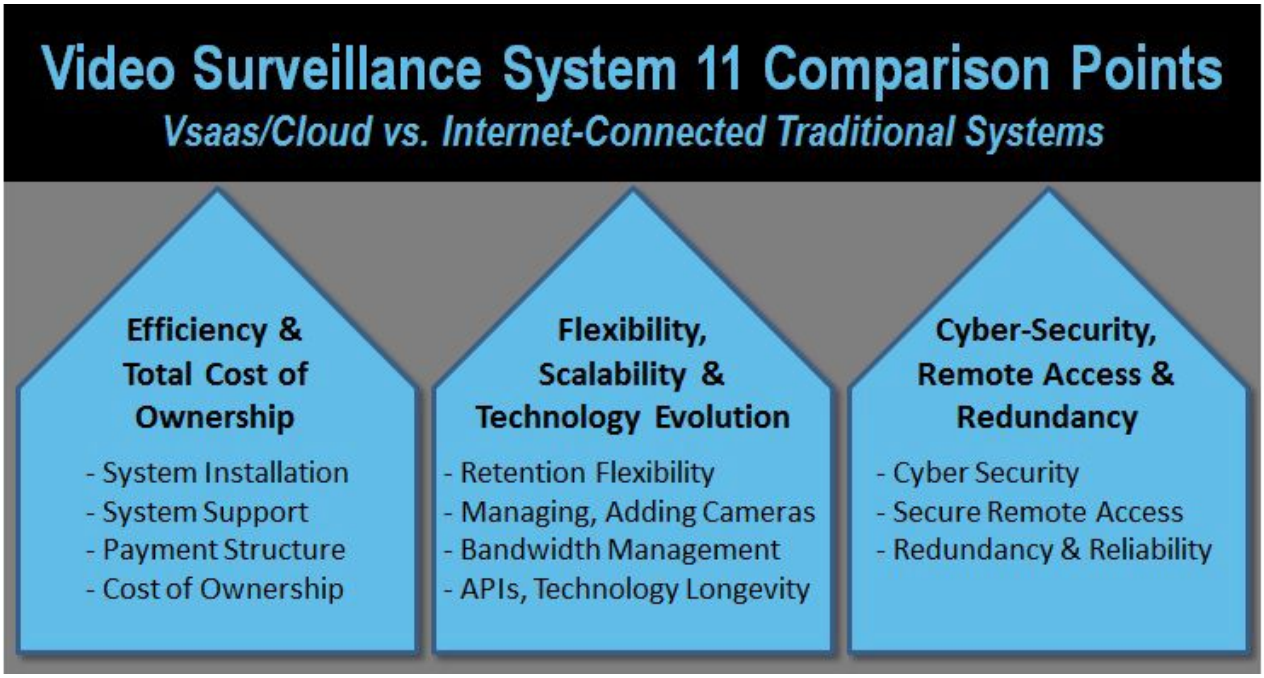
With a true cloud solution, the video processing and management is performed by the cloud. The system may have an onsite device to communicate with the cameras and the cloud, but the device is simple and acts as a communications conduit.

3. ELEVEN POINTS OF COMPARISON: VSAAS/CLOUD VS. TRADITIONAL

In the point-by-point comparisons below, we use the features associated with more advanced cloud surveillance systems, emphasizing areas on where there are the greatest differences between systems.

These comparisons can serve as a foundation checklist when you are comparing systems and assessing which best meets your needs. You can use the list to compare:

- Cloud systems vs. internet-connected traditional systems.
- Levels of robustness between cloud systems. Even with VSaaS offerings, there can be a range of the features and functionality.



Efficiencies & Total Cost of Ownership

3.1 SYSTEM INSTALLATION

Internet-Connected Traditional DVR/NVR/VMS	*Cloud-based VMS / VSaaS*
Deploying a traditional system is a long, complex process. You must install the operating system software, configure your routers, set up storage servers, configure your cameras, and install the application software.	A cloud-based system has on-demand deployment. You plug in the on-premise bridge appliance and can auto-configure your cameras. (Additional information on camera management and support can be found in section 3.6.)

3.2 SYSTEM SUPPORT

Internet-Connected Traditional DVR/NVR/VMS	*Cloud-based VMS / VSaaS*
It is a manually intensive process to support and maintain the on-site hardware and software, firmware and configuration updates.	Because the compute-heavy hardware and software are 'in the cloud', with only an on-site bridge appliance to connect the cameras to the cloud-based VMS, the ongoing support is done off site by the provider.

3.3 PAYMENT STRUCTURE

Internet-Connected Traditional DVR/NVR/VMS	*Cloud-based VMS / VSaaS*
The systems have a high up-front capital expense for the system hardware and software. Ongoing support expenses can be unpredictable.	The 'Video Surveillance as a Service' model has an extremely low up front capital expense, along with a predictable monthly operating cost.
Goals not aligned, due to prevalent "pay when it breaks" approach. The hardware pricing is uneven as the company scales and needs more cameras and storage.	The integrator and customer's goals are aligned, with pricing based on a pay as you go for what you use" via a monthly subscription fee based on number of cameras and retention period. The system grows with the customer's business.

3.4 TOTAL COST OF OWNERSHIP

Internet-Connected Traditional DVR/NVR/VMS	*Cloud-based VMS / VSaaS*
The initial cost is high, including high cost hardware/software, and installation. The ongoing costs include: an annual maintenance fee, Router configuration, System Configuration & Operating System backup, OS security patches, Remote network access, IT staff time, Space, Power, Tampering repairs, Training staff for retrieval, SW update installation, PC client SW install/upgrades, Central management, Redundancy, Mobile apps, Video backup, Cyber security expertise & support, and Multi-site integration.	The initial cost is low, typically a low cost bridge appliance. When all costs are factored in, the ongoing monthly subscription costs are lower due to the economies of scale from the shared cloud infrastructure and support. These elements are discussed in more detail in other sections.

Flexibility, Scalability & Technology Evolution

3.5 STORAGE RETENTION FLEXIBILITY

Internet-Connected Traditional DVR/NVR/VMS	*Cloud-based VMS / VSaaS*
A traditional DVR, NVR or VMS, will store the video on-site. The storage retention is rigid, as you are limited by hardware capacity you chose when you purchased and installed your system. If you want to increase the resolution or retention period of your cameras, you must buy additional or replacement hardware and configure it.	Advanced cloud systems offer a flexible combination of on-premise and cloud storage. You get same smooth access regardless of where the video is viewed or stored. Ask your provider, as some systems where the camera talks directly to the cloud, cannot store video on-premise. You can instantly increase resolution or retention period, without having to modify your existing hardware. Because cloud systems utilize a large shared cloud infrastructure for video storage, they provide tremendous economies of scale and flexibility.

3.6 ADDING & MANAGING CAMERAS

Internet-Connected Traditional DVR/NVR/VMS

The systems typically support a broad array of analog & IP camera choices.

Once initial camera wiring is complete, users must manually connect & configure new cameras.

Cloud-based VMS / VSaaS

AAdvanced cloud systems also support broad array of analog & IP camera choices.

Once the initial camera wiring is complete, cameras are configured automatically. Dashboards show camera status with instant alerts for camera or internet issues.

3.7 BANDWIDTH MANAGEMENT

Internet-Connected Traditional DVR/NVR/VMS

Bandwidth required for remote viewing. On-site video recording storage requires no bandwidth.

Cloud-based VMS / VSaaS

Bandwidth required for remote viewing. On-site video storage buffering requires no bandwidth - but majority of storage is streamed, requiring bandwidth. Some cloud systems have highly advanced bandwidth management to reduce consumption & provide smoother remote viewing.

3.8 TECHNOLOGY LONGEVITY, APIs

Internet-Connected Traditional DVR/NVR/VMS

Traditional systems have a shorter time to obsolescence. They may start with robust features, but there core feature set is fixed at time of hardware purchase. You can download firmware updates, but limited ability for technology updates. Plus updates are manual & support intensive.

APIs are closed and generally require signing an NDA. API functionality is limited.

Cloud-based VMS / VSaaS

Rapid technology evolution. Provider sends automatic technology updates through the internet to your on-site appliance. Your system is continuously evolving for new innovations, has longevity.

APIs for analytics, integration & applications are open and publicly published. Fully functional APIs can be used in other systems.

Cyber-Security, Remote Access & Redundancy

3.9 CYBER SECURITY

Cyber-security is top of mind for management. Cyber-security is a double threat for cyber security, both for the physical security system itself and as an attack vector to rest of network.

We have a detailed white paper on Cyber-security best practices for video surveillance for cloud and internet- connected traditional systems.

Internet-Connected Traditional DVR/NVR/VMS

End user requirements for remote access to their videos have resulted in traditional DVRs, NVRs and VMS's typically being connected to the to internet by the integrator or installer for remote video access. The result is the need to install and configure firewall.

The end customer then monitors for attack vector vulnerabilities such as: operating systems, open ports, on-site vendor software.

Cloud-based VMS / VSaaS

Advanced cloud-based video management systems do not have the cyber-security vulnerabilities of traditional systems. There are no open ports, no on-site firewalls, and no on-premise software. No firewall installations are required.

Some cloud VMS vendors have dedicated cyber security teams to monitor new vulnerabilities, such as Ghost and Heartbleed, and apply instant security patches via the cloud to the on-premise appliance.

3.10 REMOTE ACCESS

Internet-Connected Traditional DVR/NVR/VMS

With traditional systems, remote video access was typically not architected into the original system, but rather added on due to customer requirements. The quality of video access can be unpredictable, with choppy streaming and poor image quality. Additionally, encryption is rare, creating privacy concerns. Browser Incompatibilities are common.

Cloud-based VMS / VSaaS

Cloud-based systems were architected for remote access. Advanced systems have smooth video access & streaming.

Additionally, some provide encryption at rest & in transit. Universal web browsers support and mobile apps are common.

3.11 REDUNDANCY & RELIABILITY

Internet-Connected Traditional DVR/NVR/VMS	*Cloud-based VMS / VSaaS*
Traditional DVRs, NVRs and VMS's have highly variable redundancy levels. Further, internal IT staffing is required to maintain the redundancies. The duplicate servers are often idle, adding to the overhead expense.	Cloud data centers have double and triple redundancy. The shared infrastructure results in fullserver utilization and economies of scale. Advanced cloud systems provide a couple of days of on-premise storage as a back-up to protect against the internet going down, along with instant alerts.

4. CONCLUSION

Following the well-established trend of other industries, video surveillance is moving to the cloud.

The primary functionality drivers include rapid technology evolution, cyber security, retention flexibility, smooth remote access, and other factors.

Financial consideration are the reduced capital expenses and lower total cost of ownership due to economies of scale. Further, the pay only for what you use 'as-a-service' payment model better aligns end customers, security integrators and system vendors for ongoing support and the growth and evolution of the customer's business.

More efficient and effective management come in the form of on-demand deployment, superior multi-site integration and management, and instant system alerts, such as for offline cameras.

ELEVEN POINTS OF COMPARISON: VSAAS/CLOUD VS. TRADITIONAL			
Efficiency. Cost of Ownership.			
	Task	**Internet-Connected Traditional**	**VSaaS/Cloud System**
	Fundamental	The video processing and management occurs on a system installed at your site. This video may be later accessed via an internet connection for viewing or archival storage.	May have an onsite device to communicate with the cameras and the cloud, but video processing and management is performed by the cloud. The onsite device is simpler and acts as a communications conduit.
1	**System Installation**	Long, complex process. Install OS SW, configure routers, set up storage servers, configure cameras, install application SW.	On-demand deployment. Plug in the Bridge. Auto-configure cameras.
2	**System Support**	Manual, support intensive	Automatic cloud updates, Economies of scale
3	**Payment Structure**	High up-front capital expense for system HW & SW. Ongoing support expenses can be unpredictable. Goals not aligned, due to "pay if/when it breaks" approach. HW pricing is uneven as the company scales & needs more cameras and storage.	Low up front capital expense & predictable monthly operating cost. The integrator and customer's goals are aligned with the "as-a-service" model, The pricing is based on a "Pay as you go for what you use" via a monthly subscription fee based on number of cameras and retention period. The system grows with the company.
4	**Total Cost of Ownership**	Initial Cost: High cost HW, SW installation. Ongoing Costs: Annual maintenance fee, Router configuration, System Config & Operating System (OS) backup, OS security patches, Remote network access, IT staff time, Space, Power, Tampering repairs, Training staff for retrieval, SW update installation, PC client SW install/upgrades, Central management, Redundancy, Mobile apps, Video backup, Cyber security expertise & support, Multi-site integration.	Initial cost: Low cost hardware bridge. Ongoing costs: When all costs are factored in, the monthly subscription costs are lower due to the economies of scale from the shared cloud infrastructure and support. Many of these individual cost elements are discussed in more detail in other sections.
Flexibility. Scalability. Technology evolution.			
	Task	**Internet-Connected Traditional**	**VSaaS/Cloud**
5	**Storage Retention Flexibility**	Video stored on-site. Storage retention is rigid - limited by hardware capacity when system purchased and installed. To increase the resolution or retention period of your cameras, you must buy additional or replacement hardware and configure it.	Advanced cloud systems offer flexible combination of on-premise and cloud storage. Same smooth access regardless of where the video is viewed or stored. (Ask your provider, as some systems where the camera talks directly to the cloud, cannot store video on-premise.) Economies of scale and greater flexibility from large shared cloud infrastructure for video storage. Resolution or retention period can be increased in real-time, without having to modify your existing hardware.

6	**Managing & Adding Cameras**	Support broad array of analog & IP camera choices. Once initial camera wiring is complete, users must manually connect & configure new cameras.	Support broad array of analog & IP camera choices. Once initial camera wiring is completely, cameras are configured automatically. Dashboards show camera status with instant alerts for camera or internet issues.
7	**Bandwidth Management**	Bandwidth more available/affordable. Bandwidth required for remote viewing. On-site video recording storage requires no bandwidth. Th	Bandwidth more available/affordable. Bandwidth required for remote viewing. On-site video storage buffering requires no bandwidth - but majority of storage is streamed, requiring bandwidth. Some cloud systems have highly advanced bandwidth management to reduce consumption & provide smoother remote viewing.
8	**APIs, Technology Longevity**	Faster obsolescence. May start with more features, but core feature set is fixed at time of hardware purchase. You can download firmware updates, but limited ability for technology updates. Plus updates are manual & support intensive. APIs are closed, and generally require signing an NDA. API functionality is limited.	Rapid evolution. Provider sends automatic technology updates through the internet to your on-site appliance. Your system is continuously evolving for new innovations, has longevity. APIs for analytics, integration & applications are open and publicly published. Fully functional APIs can be used in other systems.
Cyber-security, Remote Access, & Redundancy			
	Task	**Internet-Connected Traditional**	**VSaaS/Cloud**
9	**Cyber-Security**	Typically connected to internet by the integrator or installer to provide remote video access. Need to install/configure firewall. End user monitors for attack vector vulnerabilities such as: operating systems, open ports, on-site vendor SW.	Cloud vendor vulnerability monitoring by dedicated security team. Instant security patches via the cloud to on-premise appliance. No open ports, no on-site firewalls, no on-premise SW. No firewall installation necessary.
		Detailed whitepaper on Cyber-security best practices for video surveillance for cloud and internet-connected traditional systems:	
		www.eagleeyenetworks.com/security-camera-system-cyber-best-practices	
10	**Remote Access**	Remote video access was typically not architected into the original system; instead is an add-on, so video access can be choppy. Encryption rare. Browser Incompatibilities common.	Architected for remote access. Advanced systems have smooth video access & streaming. Some provide encryption at rest & in transit. Universal web browsers support and mobile apps are common
11	**Redundancy & Reliability**	Variable redundancy levels. Internal IT staffing required to maintain, Duplicate HW idle often, adding to overhead expense.	Cloud data centers have double and triple redundancy. The shared infrastructure results in full server utilization and economies of scale. Advanced cloud systems provide a couple of days of on-premise storage as a back-up to protect against the internet going down, along with instant alerts.

ABOUT DEAN DRAKO, CEO OF EAGLE EYE NETWORKS

Dean Drako founded Eagle Eye Networks in 2012 as the first cloud-based video surveillance company to provide both cloud and on-premise recording. In 2015, Eagle Eye Networks was named to CSO Outlook's "10 promising cloud security providers".

Previously, as founder, president and CEO of Barracuda Networks, Dean created the industry's first email security appliance in 2003 and subsequently grew the company to more than 140 products, 150,000 customers and approximately 1000 employees.

Dean is also the owner and Chairman of Brivo, a cloud access control company. Dean was previously the founder of Boldfish, a leading provider of enterprise messaging solutions that was acquired by Siebel Systems in 2003. Dean was founder, President and CEO of Design Acceleration, Inc (DAI), a maker of superior design analysis and verification tools, which was acquired by Cadence Design Systems in 1998. Dean received his BSEE from the University of Michigan, Ann Arbor and MSEE from the University of California, Berkeley.

Goldman Sachs named Dean as one of the "100 Most Intriguing Entrepreneurs of 2014."