



BEST PRACTICES GUIDE

Video Security Primer

9 Core Elements That Ensure Businesses Have the Best System for Their Needs



TABLE OF CONTENTS

The Nine Core Elements	2
1. Cloud for Video Surveillance	3
2. Camera Flexibility	4
3. Ease of Use	5
4. Cybersecurity	8
5. Total Cost of Ownership	10
6. Bandwidth Management	11
7. More than Just Security	12
8. Service and Support	13
9. Innovation and Future-Proof Development	
The Bottom Line	16

Today's video management system (VMS) is not your simple solution of the past. Gone are the days when the VMS was used solely for surveillance and security.

A modern cloud-based system goes far beyond that, providing analytics and business intelligence to make your organization smarter and more efficient, and your business a safer place.

Whether you're trying to create a more customer-centric restaurant, efficient retail operation, safe gym environment, or healthy campus, a true cloud VMS can be paramount to your success.

Who Will Benefit From This Guide?

Eagle Eye Networks experts speak every day with people seeking to better understand cloud video surveillance, but many don't know where to begin. These individuals are often owners or operators of multisite commercial businesses who are responsible for:

- Managing 10 to 50 sites, such as retail shops, gymnasiums, and quick serve restaurants
- Operating 10 to 35 video surveillance cameras per site
- Selecting a new video surveillance system with a budget over \$75,000, or upgrading an existing system with a budget over \$25,000
- Continually finding ways to make their business more efficient, effective, and secure

If any or all of these points resonate with you, this guide to cloud video management system (VMS) key elements will serve you well. That said, everyone from small business owners to enterprise customers can glean takeaways from these pages. At a high level, this guide explains the top nine key features of a cloud video surveillance system.



1. Cloud for Video Surveillance

What exactly is “cloud computing” and how do businesses like yours use it for physical security and video surveillance? Cloud computing simply means storing and accessing data on the internet versus storing and accessing data on a computer that’s “on-premise” (installed in your business).

While the term “cloud” is often used loosely, with a true cloud video solution, the video is processed and managed in the cloud. The true cloud system may have an onsite appliance, but that appliance is simply a communication conduit that conveys information from security cameras to the cloud.

The move to cloud-based systems of all kinds, not just video surveillance, was well under way by the beginning of 2020. It’s not always obvious, but cloud systems are mainstream in most circles – for example, if you have systems that manage payroll, customer relationships, or workflows, they’re likely in the cloud. But the onslaught of COVID-19 greatly accelerated the adoption of cloud systems. In fact, research indicates the percentage of companies that have more than one critical business application in the cloud jumped from 60 percent pre-pandemic to 90 percent today. The top reason given is data access from anywhere, any time.

The global pandemic brought with it quarantines, remote work, and new ways of communicating with colleagues and customers. These changes have helped illuminate and amplify the benefits of cloud for video surveillance. Let’s take a look at how multisite commercial businesses benefit from cloud technology for video surveillance:

COST AND MAINTENANCE

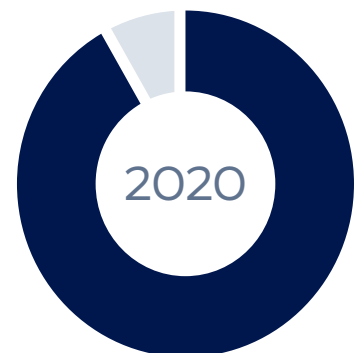
Cloud offers a much lower total cost of ownership (TCO), with substantial economies of scale. A cloud system should offer a subscription-based model, so you only pay for what you actually need and use. You can also save money by choosing a VMS partner that doesn’t lock you into purchasing its cameras. Instead, choose a VMS partner that lets you use the cameras you’ve already installed, select your preferred cameras, or use those of the cloud vendor. With cloud, the cost of maintenance is also significantly reduced. That’s because you don’t need to worry about updating your system. New features and security enhancements happen automatically. Cloud systems continuously deliver updates over-the-air.

CYBERSECURITY

With your video surveillance system connected to the internet, cybersecurity should be fully addressed by the cloud vendor, and it should provide the end user features for secure sign-in, user permissions, and audit trails if needed. System cybersecurity should include:

- Secure encryption to buffered and locally-recorded video
- Constant monitoring against threats
- No open ports or onsite firewalls
- No onsite software to patch (updates are automatic)
- Triple redundant storage for events
- Two-factor authentication

The onslaught of COVID-19 greatly accelerated the adoption of cloud systems. The percentage of companies that have more than one critical business application in the cloud jumped from 60 to 90%.



PRO TIP

Look for a Cloud That's Purpose Built for Video

There are public clouds, some of the most well-known being Amazon Web Services (AWS) and Microsoft Azure, that companies pay to store and manage their data. These public clouds cater to large numbers of users who pay as needed, but are subject to the policies and security measures implemented by the cloud provider. Then, there are private (often called hosted) clouds, such as the Eagle Eye Cloud, which is purpose-built to store and manage video.

SCALABILITY

Adding locations and cameras, increasing the number of users, adjusting camera resolution, and extending video retention periods are just some of the reasons that multisite commercial customers and others demand a scalable solution. Traditional premise-based VMS systems make it difficult to do this and lack the infrastructure and flexibility to meet these needs. Conversely, cloud-based solutions are designed to run on a scalable set of computing and network resources. With a true cloud system, it's easy to centralize your video surveillance across multiple locations, add and delete users, and adjust retention and resolution in real time.

ANYWHERE ACCESS

A well-engineered cloud VMS will include a modern mobile app so users can conveniently access video and manage features anywhere in the world with internet connectivity from their computers or mobile devices. Cloud VMS subscribers can activate features, such as video analytics, with the click of a button, without needing to install any additional software.

2. Camera Flexibility

Cameras are to your VMS as tires are to your car. Because just as a car relies on its tires to run, a VMS relies on cameras to be its source of data ... to drive security and business intelligence.

Consequently, it's important to select a cloud VMS vendor that offers you flexibility in your camera selection and management. Consider the following:

- Existing Investment**
The VMS you choose should allow you to use your existing cameras, so you don't have to rip-and-replace perfectly good equipment and buy the vendor's cameras.
- Camera Models**
If you have an existing VMS, does it use internet protocol (IP), analog, or HD over Coax cameras, or a combination of these models? If you're looking to upgrade to the cloud, the new system you choose should support the cameras you already have installed, regardless of model.
- Camera Types**
The system you select should be capable of supporting cameras other than fixed cameras, such as body-worn, vehicle, and drone-mounted cameras.
- Camera Locations**
Whether you have just one facility to secure or multiple locations, the vendor you select should be able to support your needs, even if you have outdoor locations, where extreme weather conditions could become a factor.
- Camera Numbers**
Your cloud vendor should be able to support any number of cameras.
- Accessibility**
You should have the ability to access and configure your cameras remotely.
- Camera Sharing**
Your vendor should offer the ability to give first responders real-time access to your security cameras in emergency situations.

- **Resolution**
You should be able to assign resolutions on a camera-by-camera basis.
- **Retention**
Compliance requirements that dictate camera retention times should be easily met.
- **Features**
Special camera features, such as analytics, thermal, infrared, or low-light capabilities should be readily available.



PRO TIP

Don't Get Your Hands Tied with Limited Camera Choices

The Eagle Eye Cloud VMS is camera agnostic, allowing the greatest choice and flexibility of any system on the market. It works with thousands of cameras, including IP, analog, and HD over Coax, from all the leading manufacturers. And, if you need a solution that includes cameras from the cloud vendor, Eagle Eye offers a full range of branded cameras with seamless integration to the Eagle Eye cloud.

3. Ease of Use

Ease of use should be top-of-mind when considering a cloud video surveillance offering. The technology should fit your work environment and match the technical capability of your staff. The interface should be friendly, the navigation intuitive, and the product configuration able to perform on whatever devices you prefer. You, your managers, and other employees should not have to be IT professionals to feel comfortable using the system.

This solution should offer:

EASY INSTALLATION

Just plug in the on-premise appliance and auto-configure your cameras. There should be no need to configure firewalls or routers.

SIMPLE CONFIGURATION

Your local appliance should automatically detect your cloud video cameras and configure the network appropriately. It should take a single click to add a camera. The resolution and frame rate of these cloud security cameras should be automatically set, based on the camera profile.

SINGLE SIGN-ON

Single sign-on (SSO) is an authentication service that permits a user to leverage one synchronized set of credentials to access the organization's entire suite of applications. Modern surveillance systems may also offer Apple Touch ID fingerprint biometrics for ease of sign-in and enhanced security.

ATTRACTIVE AND INTUITIVE INTERFACE

You want your video surveillance application to be highly intuitive, as that's what you've likely grown accustomed to with your personal apps. It should enable you to use native iOS and Android gestures, for example, pinch-spread and double-tap control zooming.

CENTRAL MANAGEMENT

Select a system that allows you to easily delegate access, revoke access, and track user activity of the cloud VMS from your web browser. This is especially important in industries with high turnover, seasonal surges, or transient workforces.

MULTI-SITE VIEWING

Monitor multiple sites in a single interface, with the ability to view real-time or recorded video from your desktop or mobile device and scroll and zoom to different locations.

PRE-SET LAYOUTS ACROSS SITES

Robust geographic maps allow users to create custom floor plans, drag and drop cameras to specify their location, and much more. You should even be able to create layouts that show video from different locations on the same screen. For example, you could choose to view all cash registers at the same time, even if the stores are scattered across the country.

ON-THE-FLY CAMERA SHARING

A system that supports rapid camera sharing with authorized users and first responders offers an efficient and easy way to improve response times, mitigate loss, and quickly address other business issues.

Plug and Play Configuration with Eagle Eye

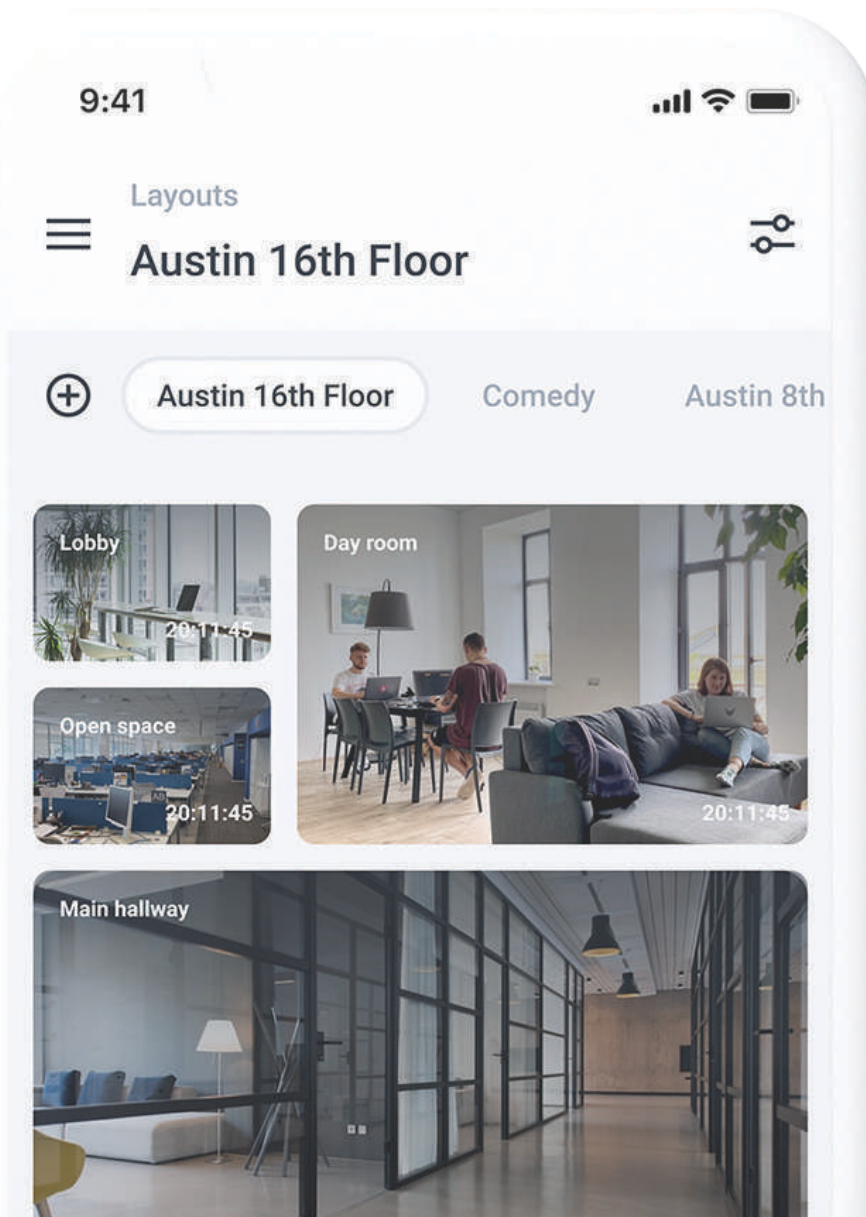


STORAGE RETENTION AND FLEXIBILITY

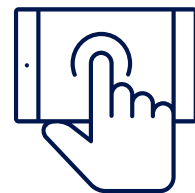
Advanced cloud systems offer a flexible combination of on-premise and cloud storage. You get the same smooth access regardless of where the video is viewed or stored. Ask your provider, as some systems where the camera talks directly to the cloud can't store video on-premise. You can instantly increase resolution or retention periods, without having to modify your existing hardware. Because cloud systems use a large shared cloud infrastructure for video storage, they provide tremendous economies of scale and flexibility.

INVESTMENT PROTECTION

You've made a big investment in a security system and you expect it to last. You want your video surveillance system to operate optimally even as business environments change, such as regulatory requirements, or societal issues, such as pandemics or social unrest. And, you want upgrades to the system to be quick and easy. With a traditional VMS, an upgrade generally requires additional (often substantial) investment and/or making an appointment with a security installer to visit all of your business locations in person to make changes and swap out devices. Cloud technologies, on the other hand, can be upgraded, kept current, or modified to meet changing needs without replacing parts or an entire system.



Create custom layouts and navigate using iOS and Android gestures, for example, pinch-spread and double-tap control zooming.



Computer and network security focuses on protecting the confidentiality, integrity, and availability (CIA) of the networked systems and the data they contain. These three factors are paramount for video systems.

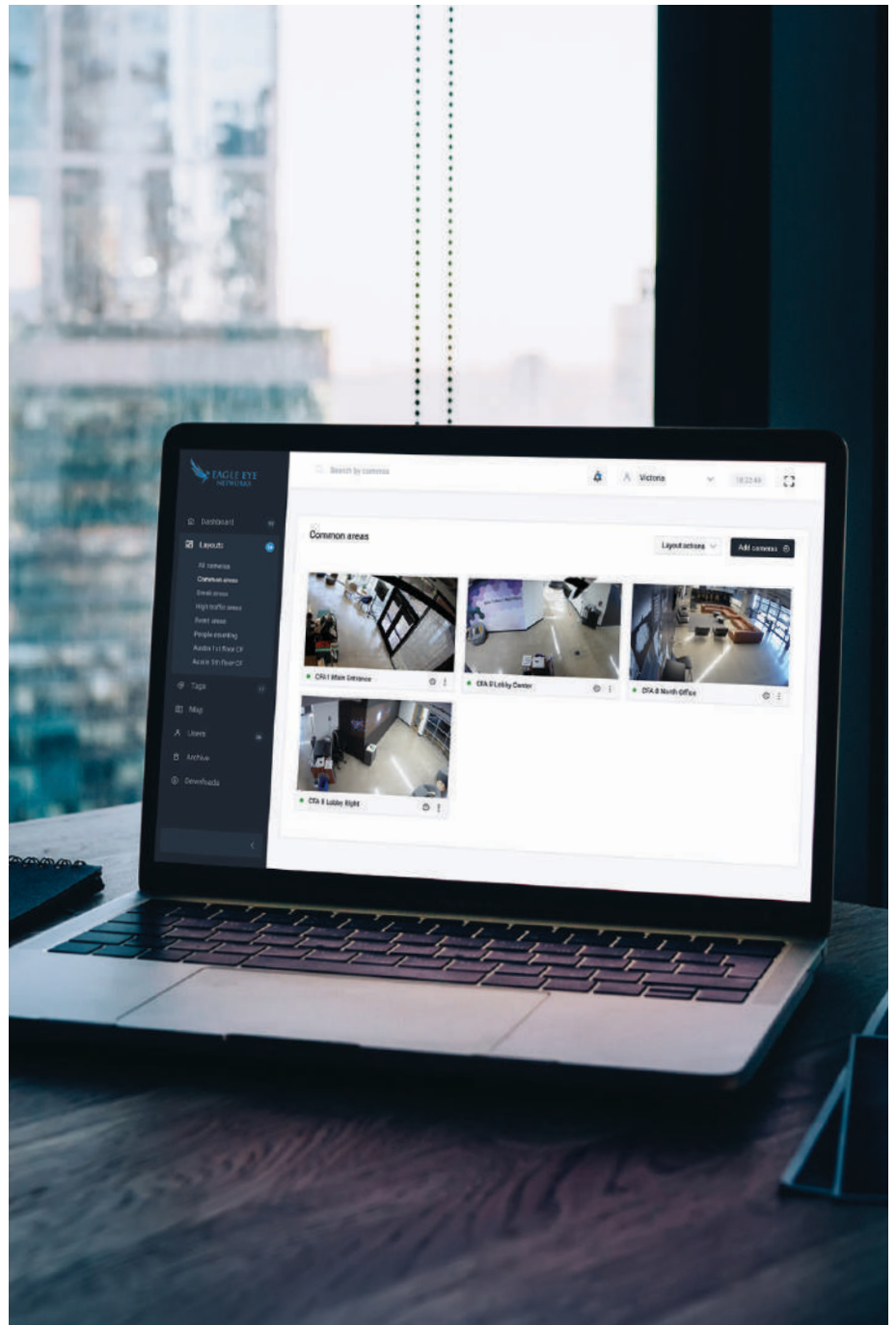


4. Cybersecurity

Cybersecurity best practices are essential to protect your business, employees, and profits. Fortunately, true cloud systems come with cybersecurity built in.

Computer and network security focuses on protecting the confidentiality, integrity, and availability (CIA) of the networked systems and the data they contain. These three factors are paramount for video systems, given the potential for any camera's recorded video to become critical legal evidence.

However, for most video systems, internet connectivity puts confidentiality, integrity, and availability at risk, because most systems don't have built-in protections against cyberattacks. Thus, many video systems are defenseless, even though cybersecurity attacks are on the rise.



To safeguard your system and the data it contains, look for the following cybersecurity features and functionality:



STRONG ENCRYPTION

Encryption is the process of changing data so it's unreadable (encrypting), in a way that it can be changed back into its readable form (decrypting). The simplest kind of encryption uses a single set of characters (numbers, letters, and/or symbols) – the encryption key – to both encrypt and decrypt the data.



CONSTANT MONITORING AGAINST THREATS

Encryption is the process of changing data so it's unreadable (encrypting), in a way that it can be changed back into its readable form (decrypting). The simplest kind of encryption uses a single set of characters (numbers, letters, and/or symbols) – the encryption key – to both encrypt and decrypt the data.



TRIPLE REDUNDANT STORAGE

Recorded video should be protected against loss by fully redundant video storage (triple redundancy is best). A cloud-based VMS's data centers should have double and triple redundancy. Advanced cloud systems provide several days of on-premise storage as a backup to protect against the internet going down.

For both on- and off-premise recording, cameras should never connect directly to the internet.



NO OPEN PORTS OR ONSITE FIREWALLS

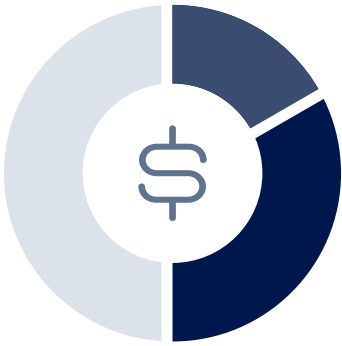
For both on- and off-premise recording, cameras should never directly connect to the internet. For off-premise recording, appliances should aggregate and buffer the video data for secure encrypted transmission to the cloud. For on-premise recording, cloud-managed video recorders (CMVRs) should record locally and continue to ensure cameras have no direct link to the internet.



TWO-FACTOR AUTHENTICATION

Two-factor authentication should be used to provide strong security by establishing trusted user devices (PCs, laptops, tablets, and smartphones) and only allowing camera and video access from those trusted devices. Attempts to sign in using a non-trusted device should result in denial of access.

Moving computing and video storage infrastructure to the cloud results in overall savings between 20 and 50% compared to a typical onsite system.



5. Total Cost of Ownership

Operational costs, many of which are not in plain sight, can significantly raise the cost of technology ownership. However, cloud computing has changed the total cost of ownership (TCO) landscape for security video surveillance. Moving the computing and video storage infrastructure to the cloud results in a total cost of ownership considerably below a typical onsite system. The savings generally range between 20 and 50 percent compared to costs for hosting the VMS applications in a corporate data center (whether in-house or third-party operated).

The typical advantages of cloud-based over data center-based video management systems include:

- A lower total cost of ownership.
- Lower upfront expenditure costs.
- Data storage and video recording and processing are fully redundant.
- Strong cybersecurity, including data encryption in transit and at rest.
- Better wide-area mobile device performance without the need to open ports on the firewall.
- Automatic security and feature updates with no action needed by the service provider.
- The ability to add and subtract video analytics and other system capabilities on-demand, paying only for the period in which they're used.
- Freedom to expand video retention and recording resolution and frame rate on a per-camera basis, without having to make any on-premise infrastructure changes.
- A fully operational system during upgrades to server, operating system software, application software, and computing and storage hardware. Downtime is eliminated from security/bug fix updates, software version updates, and server hardware refreshes.
- Continuous delivery software engineering, which provides incremental software improvements in intervals of weeks, rather than months or years. Incremental improvements eliminate staff learning curves that often occur with typical client-server software update cycles. Additionally, all subscribers are always using the very latest set of features and capabilities.
- No need to increase the IT department's workload by requiring them to manage a rack of gear for video management, allowing them to focus on core business operations.
- Less inter-department approval and red-tape barriers between security and IT teams.
- Remote connectivity and download options that surpass an on-premise video management solution.

6. Bandwidth Management

Bandwidth refers to the available speed of your internet protocol (IP) network. When you look at your upload and download speeds, you're seeing your bandwidth. The more bandwidth you have, the faster those upload and download speeds. Everyone has different bandwidth, and access to high internet speeds is not yet universal.

Bandwidth requirements for a VMS differ for every user, because they're determined by three factors: camera count, recording resolution, and motion activity. Your video surveillance system vendor should build tools into the system to help you deal with the reality of bandwidth limitations and unpredictability.

PRO TIP

Manage Your Bandwidth in Low Bandwidth Scenarios

Eagle Eye Networks has developed Intelligent Bandwidth Management™ technology in its cloud security camera system to deal with the reality of limited bandwidth. For years, cloud video surveillance systems faced challenges with bandwidth consumption, but Eagle Eye's unique and multi-layered bandwidth management technology means the system works with both small and large cloud security camera installations, regardless of your internet.

The tool makes it easy for you to determine how much bandwidth the Eagle Eye Cloud VMS is using and when it's using it. For example, during business hours, bandwidth usage is often stretched thin to accommodate everyone on site. In this case, you can tell the system to only move video footage to the cloud after hours, when bandwidth is more readily available, resulting in minimal impact on your operations.

Using the Intelligent Bandwidth Management System, you can determine:

- Percentage of available network
- Fixed amount of bandwidth
- Schedule for video transmission

You'll always have access to your preview stream in real time, no matter what; but these tools will help you effectively manage the upload of your high-resolution video to the cloud.



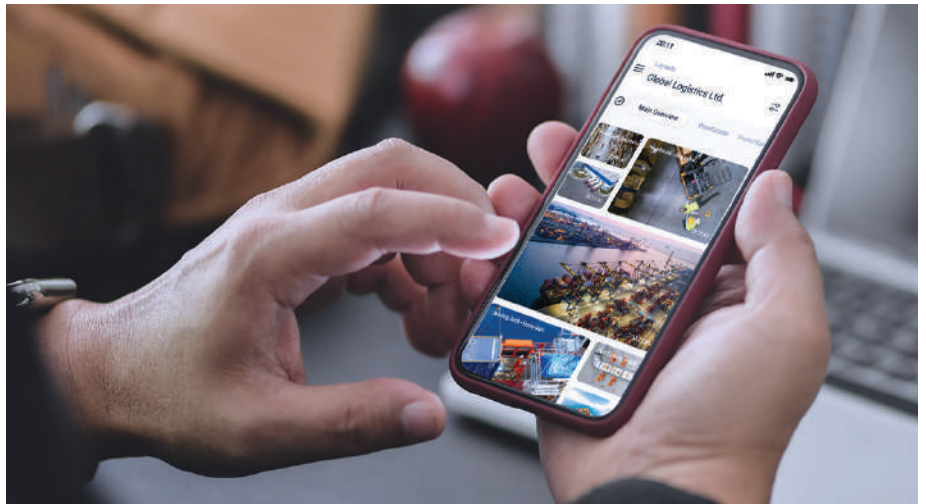
7. More Than Just Security

Artificial Intelligence (AI) for video surveillance uses software applications to analyze the audio and video from cameras to recognize humans, objects, vehicles, events, and more. In short, video analytics can analyze the data from your video source and correlate it with the scenarios and models you've set up for it to detect.

And, while video analytics provide significant benefits to businesses for security purposes, they also turn the video security system into a tool for business optimization.

Many industries are now realizing the potential of video analytics with their video surveillance systems. Owners and operators can create long-term strategies based on the insights gained from their video analytics. For example, retail shop owners can determine the number of people entering and exiting the property at any given time. Monitoring the traffic flow of customers and patterns of the establishment is crucial to operations and marketing, allowing better planning around staffing and floor layouts.

Many industries are now realizing the potential of video analytics with their video surveillance systems. Owners and operators can create long-term strategies based on the insights gained from their video analytics.



Video analytics also provide insight into employee behavior. Are proper procedures being followed? Are customer interactions positive? This can highlight areas where further training may be needed or a change in policy is required.

Employee theft is one of the biggest issues management faces within the restaurant and retail spaces. With some systems, you can integrate your point-of-sale (POS) and video surveillance to view sale and payment data in one place. Owners and operators can quickly and easily search transactions and view the video tied to events, streamlining investigations into suspicious transactions.

False alarms are another challenge, leading to false dispatches and unwanted and costly false alarm fines and citations. One of the most important AI applications is the reduction of false alarms, for example, determining a construction site “intruder” is not a thieving person, but a foraging raccoon.

The architecture for video analytics runs in one of two ways: cloud processing or edge processing. Cloud processing is when video analytics are run in the cloud. Edge processing refers to video analytics run on the camera itself. Both the physical architecture and the scenarios you need to detect and monitor will determine the right analytic for you.

8. Service and Support

When purchasing a VMS, you should inquire about vendors' service offerings. Do they offer basic service and support, such as publishing a knowledge base, hosting a user community, and providing ongoing training opportunities? Do they offer white glove support that goes beyond VMS installation and deployment? Do they support the end user, as well as the dealer/reseller?

What you want to avoid is partnering with a video surveillance provider that is all about the sale and not the service. Instead, you want to align with a vendor that will actively monitor your cameras and system to verify continuous operation. The vendor should either attempt to resolve minor camera, appliance, and network issues without having to involve you, or escalate more significant issues to you and your reseller to develop a plan for resolution.

The lines of communication should always be open. Your video surveillance provider should send email notifications of any actions taken with your system, as well as notifications if cameras are disabled or tampered with. Your vendor should also make recommendations on camera and system adjustments to help you optimize performance.

PRO TIP

You Deserve White Glove Service

Eagle Eye Networks offers a Premium Support Subscription, designed to provide the highest level of support for customers with complex environments or who need mission-critical health monitoring.

Premium Support helps you mitigate risk and protect your technology investment. This industry-leading support package includes:

- 24x7 phone support for all standard and advanced features
- Eagle Eye health monitoring of bridges and cameras with proactive contact if anything is amiss
- Advanced notification of planned features and product roadmap updates
- Weekly email updates of all outstanding support issues
- Dedicated support experts with ongoing context about customers' businesses
- Dedicated support hub with ticket tracking
- Scheduled firmware upgrades and priority access to beta programs
- Priority escalation procedures to solve complex problems

When purchasing a VMS, you should inquire about vendors' service offerings and avoid partnering with a video surveillance provider that is all about the sale and not the service. The lines of communication should always be open.



The development of cloud-based video surveillance applications is transforming systems from simple motion-based alerting devices to unified proactive and preventative solutions.

9. Innovation and Future Proof Technology

Many of today's legacy video surveillance systems require monotonous monitoring or a meticulous manual review after each triggered event to extract useful information. This places serious limitations on the effectiveness of the technology and the ability to more broadly apply it to real-world security, safety, and business challenges.

However, the development of cloud-based video surveillance applications – powered by artificial intelligence and video analytics – is disrupting established approaches and transforming systems from simple motion-based alerting devices to unified proactive and preventative solutions.

You want to ensure your system is future-ready; one that gives you the power to innovate at scale and keep pace with continuous feature and AI enhancements delivered in the cloud. Your video management system partner should be engineering the means for current deployments to accommodate planned and likely future integrations with support for infrastructure expansion and advanced application capabilities.

PRO TIP

Prepare Today for Tomorrow's Technology

5G is the fifth and next generation of mobile communication technology. It presents tremendous opportunity for the video surveillance industry.

5G gives us the ability to pull video and data from countless devices – not only from fixed video security cameras, but also mobile video devices like body cams (on bus drivers, train conductors, Uber Eats drivers, etc.) and drones, which will be particularly powerful for customers in agriculture, oil and gas, and sporting arena management.

With 5G, each video surveillance device can have its own connectivity to the cloud, so there's no local interference – which is a gamechanger from a cybersecurity perspective. In addition, 5G frees users from all the hassles associated with connectivity and bandwidth. On the backend you could be working with multiple connectivity providers – like your cellphone when it's on roaming. Also, if you wire your devices and the fixed network fails, you can use the 5G network as a reliable backup.

And, probably most exciting, artificial intelligence (AI) can be applied to large volumes of data being sent to the cloud with low latency, and quickly receive back relevant, actionable intelligence. This will foster the rise of "autonomous security," which is essentially technology (for example, automated robots and drones) that can perform various security and surveillance operations, including monitoring, investigating, and reporting.

BUSINESSES ARE TURNING TO OPEN APIS

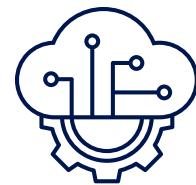
One of the best ways to ensure your system is future proofed is to choose one with an open application programming interface (API). This open interface makes it possible for two separate applications to interact and share data to create new and expanded functionality. More and more, businesses are turning to APIs to automate tasks between applications, deliver better customer experiences, and quickly innovate.

By deploying a video management system with an open API, businesses receive a host of benefits, including:

- **More Customization**
It's easy to streamline the use and management of applications, enhancing the functionality across systems.
- **Lower Total Cost of Ownership**
There is no vendor lock-in and no additional licensing fees for integrating outside applications.
- **Better Cybersecurity**
The system is able to adapt to the security needs of the organization by using industry best practices and equipment.
- **Future-Proofed Investment**
Organizations are able to integrate and incorporate tools with the video management system for all current and future needs.
- **Speed to Market**
Applications can be built in hours, not months, and updated in minutes, not weeks.



One of the best ways to ensure your system is future proofed is to choose one with an open application programming interface (API).





The Bottom Line

Multisite business owners and operators need to manage an increasing level of business complexity and change, more rapidly than ever before. Traditional commercial video surveillance is focused almost exclusively on being able to record people and property to improve security or protect those people and assets. As such, the security cameras and recording devices mattered most in the purchase of a video surveillance system. But times have changed and so too have the things you need to consider when buying a video surveillance management system.

Are you ready for a cloud VMS? Take a gut check by answering these questions:

- Q. Does my business need to improve security and operations, without increasing headcount or IT budget?
- Q. Does my VMS need to integrate with access control, point of sale, inventory, or other business-critical applications?
- Q. Does my organization struggle with inefficient processes, unsafe conditions or behaviors, higher than necessary maintenance costs, loss/theft, and/or less than desirable customer experiences?
- Q. Is our VMS providing us insights, analytics, and business intelligence to improve our bottom line and create a safer environment?

If your answer to any or all of these questions is yes, it's time to consider a true cloud VMS.

LEARN MORE

For more resources, including whitepapers, webinars, blogs, and customer success stories, please visit:

www.een.com/docs

