spot.ai

BUYER'S GUIDE

Future-proof your video surveillance

A buyer's guide to AI Camera Systems

How do you choose a video surveillance system in a noisy and fast-evolving market?

The video surveillance market is crowded, complicated and confusing. Countless players have emerged offering products that appear to be similar. The inflection of artificial intelligence with the advent of ChatGPT has added a new layer of complexity as organizations consider the role AI will play in their next video surveillance system.

You could spend months evaluating these options and navigating this complexity, *but you shouldn't.* This guide will cut through the noise and break down the considerations when thinking about how to select your next system.

Contents

1.0 Understand the landscape

1.1 Evolution of video surveillance: 2000s–2020s

The video surveillance industry has gone through several transformations since the early 2000s. Technological advancements have brought us from an analog age to a digital age, where cloud capabilities are expected and the power of AI is finally beginning to be realized.

Each new era built on the benefits of the previous one.

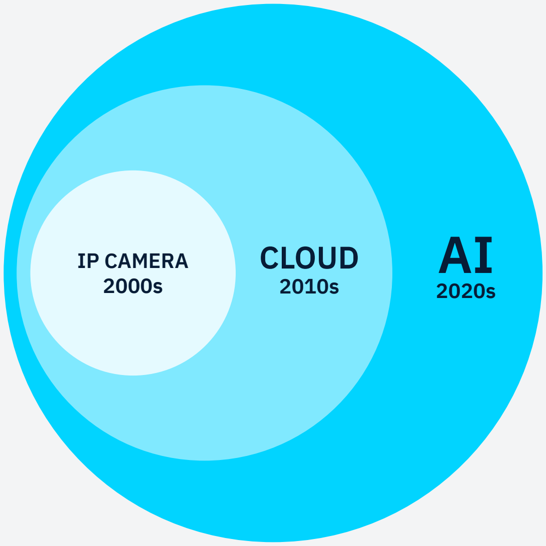


Figure A: The three Eras of Video Surveillance. Each new era built on the benefits of the previous one to expand customer value.

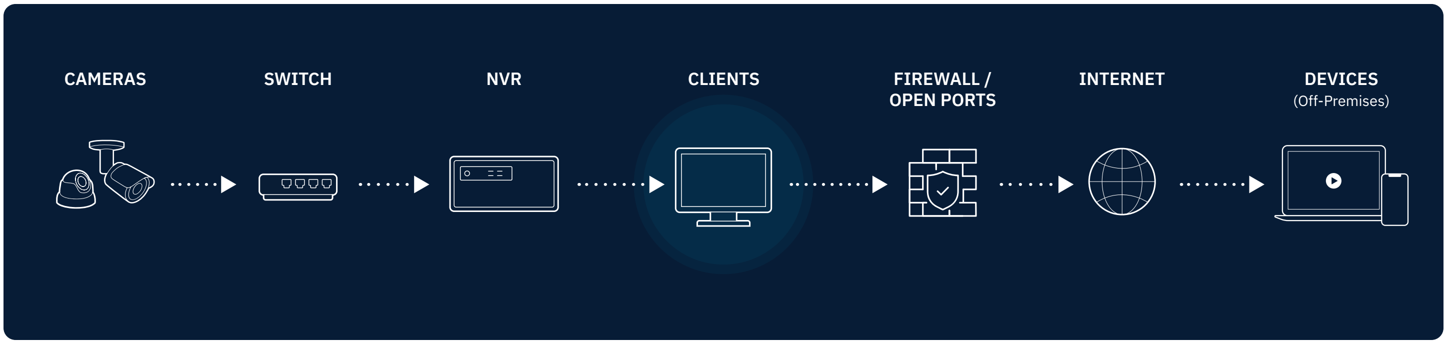


Figure B: Typical architecture of an IP camera based camera system

2000s: The era of IP cameras

Prior to the 2000s, analog cameras and VHS tapes were the primary methods of recording. The quality of these methods was limited and tapes had to be replaced frequently.

In the early 2000s, the shift to digital cameras began. Digital Video Recorders (DVRs) replaced VHS tapes, allowing for improved recording, resolution, storage, and flexibility. The introduction of Internet Protocol (IP) cameras allowed video data to be transmitted over a network. This led to the development of Network Video Recorders (NVRs), enabling remote monitoring and more efficient storage solutions.

Despite technological advancements, NVRs still presented a number of challenges. While other software applications had transitioned to the cloud, the IP Cameras lagged behind and users could only access their footage on site or remotely via a Virtual Private Network (VPN). Solutions of this kind also put the onus of system management on IT teams.

> While other software applications transitioned to the cloud, IP Cameras lagged behind.

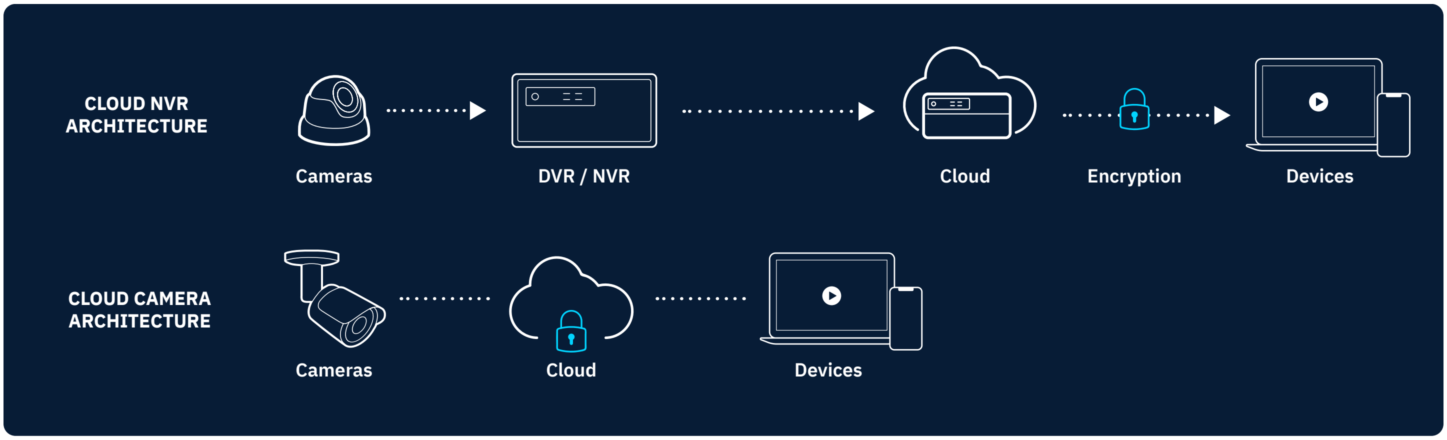


Figure C: Typical architectures of Cloud-based camera systems

2010s: The era of the Cloud

In the 2010s, cloud-based surveillance emerged, allowing businesses to store footage remotely, providing accessibility from anywhere with an internet connection. Building on this technology, two new types of solution hit the market, commonly referred to as “Cloud Cameras” and “Cloud NVRs.”

Vendors like Verkada and Rhombus led the Cloud Camera category offering a “cloud-managed” architecture that combined recording, storage, and processing on the cameras themselves, eliminating the need for DVRs and NVRs. Verkada was at the forefront of this phase, running campaigns with the message that the “NVR is dead.” This type of architecture provided benefits over the traditional DVR/NVR-based solutions, offering remote access, automatic software updates, and a modern user interface. However, these cloud camera solutions required customers to rip and replace their existing cameras with proprietary cameras, as well as large-scale upgrades to their IT infrastructure.

Vendors like Eagle Eye led the Cloud NVR category, with an architecture that allowed buyers to keep their existing cameras while still gaining the benefits of a “single pane of glass.” These solutions operate on the edge by connecting an NVR to the internet to store and process video data locally and in the cloud. The approach provided customers with the security, bandwidth, and cost benefits of an on-prem NVR, and the flexibility and convenience of the cloud. Although an NVR is still required, these solutions seamlessly enable a single pane of glass for all cameras across multiple locations while mitigating upfront costs associated with the full replacement of cameras.

Over the last decade, cloud capabilities have become an expectation. In an increasingly complex world and working environment, companies are demanding systems that are easy to install, easy to use, and easy to manage—requirements that can only be provided by the cloud.

> Over the last decade, cloud capabilities have become an expectation.

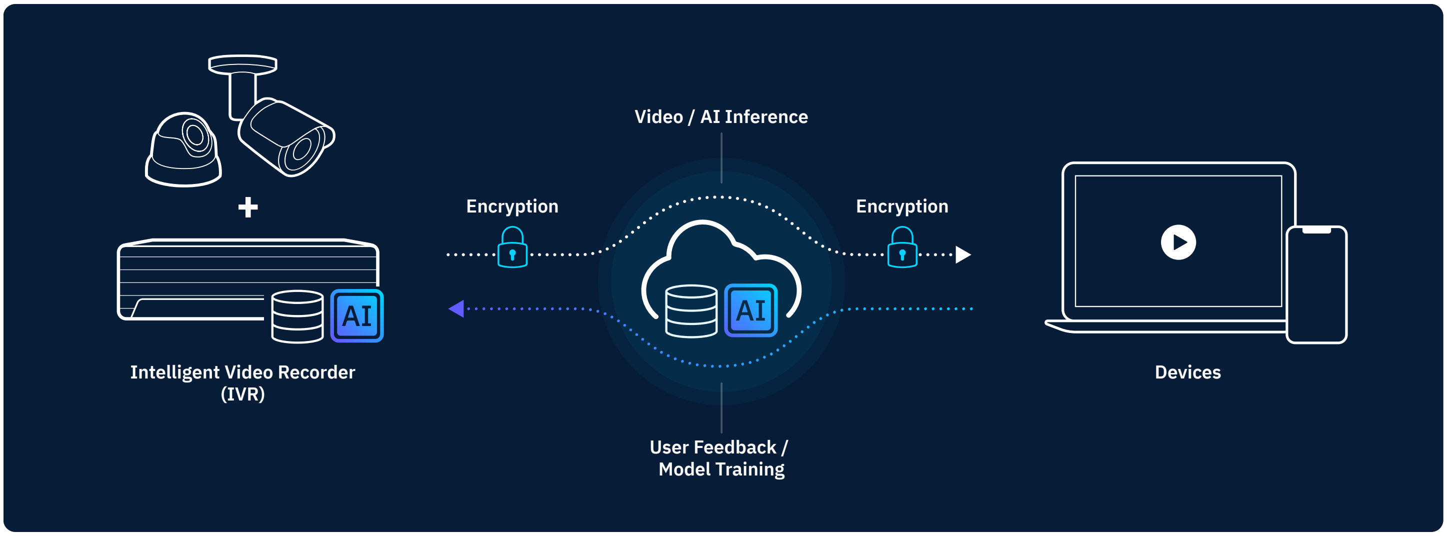

Video / AI Inference
Encryption
Encryption
AI
AI
Intelligent Video Recorder (IVR)
Devices
User Feedback / Model Training

Figure D: Typical architectures of AI Camera Systems

2020s: The era of AI

Every piece of software will get reinvented with AI, and camera systems are no exception.

We are at an inflection point where artificial intelligence is becoming increasingly powerful and useful. While the mathematical groundwork for AI models was laid in the 1950s by technology pioneers like Alan Turing, the necessary compute power to process neural network parameters wasn't developed until the mid-2000s when graphics processing units (GPUs), microchips most commonly used at the time for video games, were first used for running AI models. As GPU compute power has drastically increased in the years since. GPU performance is doubling every year. The ability to train large and complex AI models has followed in lockstep. This, along with the emergence of Foundation Models, has led AI capabilities to improve at rates faster than ever before.

These rapid improvements have led to the emergence of a new architecture of Video Surveillance products — known as “Hybrid AI” — to keep up and leverage this wave of technology transformation. Hybrid AI leverages an appliance connected to the network called an “Intelligent Video Recorder” or “IVR.” These are similar to NVRs, but have GPUs or Tensor Processing Units (TPUs) built in that allow for AI processing at the edge, as well as in the cloud.

A new set of vendors are leveraging Hybrid AI architecture and bringing “AI Camera Systems” to market. These products offer all the benefits of the cloud as a baseline, but also allows for AI applications that are performant, usable, interoperable, and scalable to accommodate the rapid developments in AI technology.

> A new architecture has emerged to keep up with the rapid improvement in Artificial Intelligence: Hybrid AI.

As AI Camera System models are entering the market, purpose built for AI, existing Cloud Camera and Cloud NVR vendors are attempting to retrofit their offerings with AI. On the surface, the products may appear similar, but it's important to understand how to cut through the marketing and select a system that meets your business needs.

	2000s	2010s		2020s
	DVR/NVR	**Cloud Cameras**	**Cloud NVR**	**AI Camera Systems**
Cameras	**Proprietary:** Camera connected directly to NVR/DVR. Analog cameras don't have to match brands with the DVR. Most IP cameras only work with the vendor's NVR.	**Proprietary:** Only vendor's cameras can be used to get access to their cloud platform.	**Open:** Work with most IP cameras on the market. Some vendors require proprietary cameras. Cameras are connected directly to the NVR.	**Open**: Work with most IP cameras on the market Some vendors require proprietary cameras. Cameras connected directly to the IVR through the local network.
Storage	**Local:** Stored on a local Hard Drive on the NVR/ DVR. Some vendors are offering cloud options but require additional software and setup.	**Cloud-native:** Stored on cameras on flash memory (SD) card and in the cloud, natively.	**Cloud-native:** Stored on the NVR on a hard drive and in the cloud, natively.	**Cloud-native:** Video is stored on the IVR on a hard drive. Vendors natively offer archiving and expandable cloud storage.
Remote Access	**Limited:** Limited remote access, often requires additional setup, opening inbound firewall ports and is subject to feature and resolution limitations.	**Native:** Advanced remote access via web browsers or dedicated mobile apps, with more features and higher resolution. Requires firewall rules to allow outbound internet access.	**Native:** Advanced remote access via web browsers or dedicated mobile apps, with more features and higher resolution.	**Native:** Advanced remote access via web browsers or dedicated mobile apps, with more features and higher resolution.
AI Architecture	**Edge-only:** No AI-specific microchips on hardware. Simple AI models run on existing processing capability of camera/NVR.	**Cloud-only:** AI-specific microchips on some hardware. Video uploaded to the cloud for AI inferences.	**Cloud-only:** No AI-specific microchips on hardware. Video uploaded to the cloud for AI inferences.	**Hybrid AI:** Purpose built with microchips to run AI models at the edge as well as in the cloud.
Cybersecurity	**Add-on:** Data is transferred through open ports and is not natively encrypted. Additional software required to secure systems.	**Native:** Natively built cybersecurity within a "walled garden" of proprietary vendor hardware.	**Native:** Cloud NVR acts as a firewall for cameras, natively encrypting video and securing cameras.	**Native:** IVR acts as a firewall for cameras, natively encrypting video and securing cameras.

Figure E: Comparison of different architectures of Security Camera Systems

1.2 AI: The next evolution of video surveillance

There are over **one billion security cameras**[1] in the world now, over double the number of cameras there were in 2015. As access to video has become more prevalent, more people are using video frequently and for much more than just security. Video use is no longer limited to reactive use by just security or IT. Professionals across the organization are using video in their day-to-day work. Camera systems have historically been used *reactively* for incident resolution. *After* an incident occurs, you search for the footage, analyze it, and share it with the appropriate parties. But with AI, camera systems are rapidly becoming powerful *proactive* tools, preventing incidents from happening in the first place.

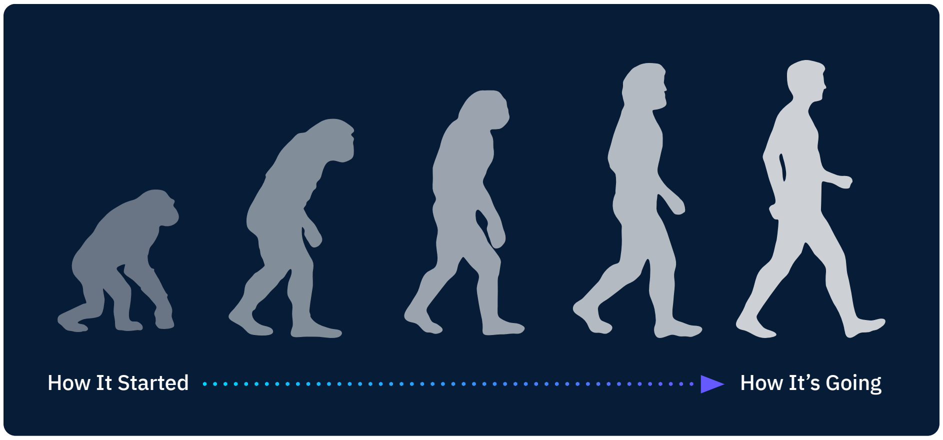


Figure F: The extent of evolution of AI from Decision Trees to Foundation Models

The dawn of open source AI foundation models has changed the landscape.

The rise of foundation models

Early AI models were hyper-tuned to specific use cases. Building the models was difficult and time-consuming because it required gathering large amounts of data, tagging the data, training the model on the data, and fine tuning the data to generate the desired results. In many cases, models were built with limited datasets. But the dawn of open source AI foundation models has changed the landscape. Foundation models have unique characteristics:

- **Powerful:** Using various methods of gathering vast datasets, like crowdsourcing, web scraping, data sharing, and simulated data, foundation models were built and made publicly available. These models are pre-trained and, because of the expansiveness of the datasets, highly adaptable to a large number of differentiated tasks.

[1] The Wall Street Journal: **'A World With a Billion Cameras Watching You Is Just Around the Corner'**

With foundation models, AI has reached orders of magnitude better performance.

- **Multimodal:** Traditionally, AI systems were designed to handle data in one specific modality. For instance, natural language processing (NLP) models primarily dealt with textual data, computer vision models focused on images and videos, and speech recognition systems processed audio data. However, in many real-world scenarios, information is presented in multiple forms simultaneously. Over time, foundation models have become increasingly multimodal, meaning they can understand and process information from multiple modalities or sources of data, such as text, images, videos, audio, and other forms of sensory inputs.

- **Self-Learning:** Technological advances have also allowed AI models to develop self-learning capabilities where the models continuously learn from inflowing data and improve their performance over time without explicit programming. This occurs through iterative cycles as the model intakes new data and adjusts its internal parameters based on the disparities between its predictions and the actual outcomes, refining its accuracy. This adaptability enables the AI to make predictions or decisions when presented with new, previously unseen data, allowing for continuous improvement as more data becomes available.

- **Accessible:** Making these models open source allows anyone to leverage and fine tune them to specific use cases with relative ease. Anyone in the world can access these powerful models and use them to solve real-world problems, leading to a surge in AI startups founded since the late 2010s.

With foundation models, AI has reached **orders of magnitude better performance**[2].

Foundation models are driving an AI revolution in every sector of the economy

AI technologies are rapidly becoming ingrained in the fibers of our personal and professional lives. Models like ChatGPT have gone mainstream and become so powerful that they are able to function like a live and helpful human assistant. With a simple one-line prompt, ChatGPT can write an entire essay in seconds, complete with cited sources. Generative AI models like Midjourney can generate completely unique works of art nearly instantly when only provided with a single phrase. Schools are leveraging AI-powered educational software to tailor lessons to the needs of individual students by adapting the level of difficulty based on the student's performance, ensuring that each student can learn at their own pace. Healthcare companies are using AI to simulate and predict the interactions between molecules in order to accelerate drug discovery. And transportation companies are using AI to optimize delivery routes and reduce fuel consumption and delivery times based on real-time traffic patterns and weather conditions.

[2] Snorkel.ai: **'Foundation Models 101: a guide with essential FAQs'**

AI is unlocking new operational use cases of video that were never before possible.

Across every industry, the immense impact of AI is already being felt, but is still largely untapped. We are entering an era of coachable AI assistants that will help with everything from marketing content creation to chatbots for customer support. We are at the forefront of an AI revolution that will impact every sector of the economy.

Foundation models are inflecting the power of AI in camera systems

The advent of foundation models has also unlocked the ability for camera systems to analyze the physical context of business environments and intelligently provide valuable visual context without the hassle of brute-forcing through a dated system. Not only is AI driving incredible and proactive automation of traditional security workflows, it is also unlocking new operational use cases at a level never before possible that help businesses generate more revenue than they previously could by automatically detecting areas of inefficiency, providing prompts on how to address them, and providing professionals in every organization insights and analytics from video data to support their day-to-day objectives.

Industry	Use Cases	Departments Using Video
Manufacturing	**Work zone safety:** Monitor whether employees are adhering to safety protocol, like wearing hard hats and safety vests in a work zone **Loading bay efficiency:** Monitor whether delivery vehicles are idling too long and compare loading time performance across locations **Production monitoring:** Monitor whether the manufacturing line equipment and crews are working effectively	EHS HR Operations IT
Auto Services	**Damage claims:** Confirm whether a vehicle was damaged prior to service by using license plate recognition to quickly locate footage of the vehicle **Throughput:** Monitor whether cars are idling too long and compare service time performance across locations **Employee training:** Use video footage to train sales reps on how to properly attend their pay stations in order to generate more revenue	Operations HR IT
Retail	**Loss prevention:** Uncover incidents of shrinkage with limited information and get proactive alerts for anomalous incidents that merit attention **Merchandise placement:** Track which items are most commonly viewed and design the space to optimize for revenue generation **Employee productivity:** Monitor whether employees are actively engaging in their assigned responsibilities	Loss Prevention Store Operations Marketing IT
State, Local, and Education (SLED)	**Campus safety:** Use facial recognition to search for known criminals on campus **Vape detection:** Use sensor integrations to detect students engaging in discouraged or prohibited behavior **Damage to facilities:** Alert when people trespass during off hours	Security Officers Principals Superintendents IT

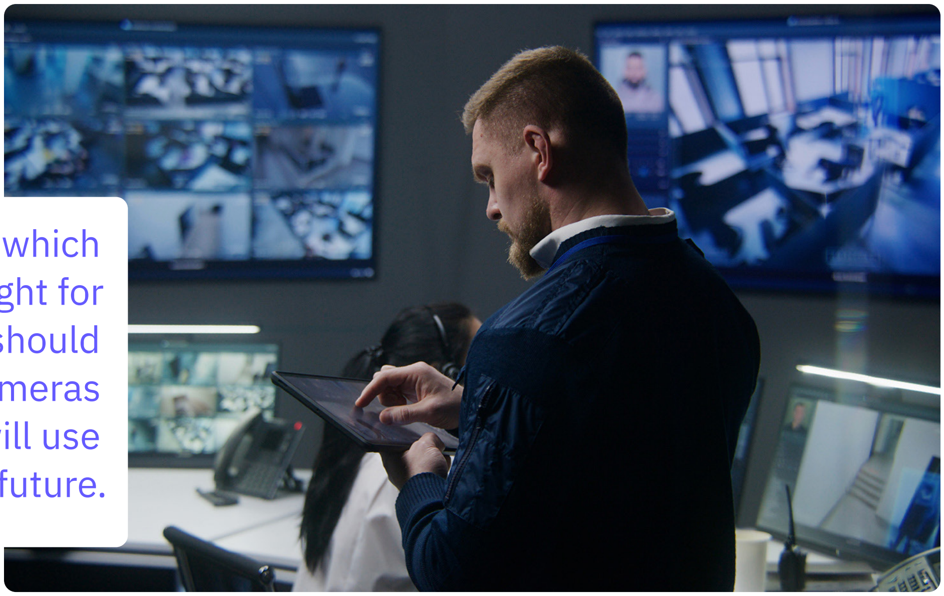
Figure G: Emerging use cases and users of video data, made possible by foundational models

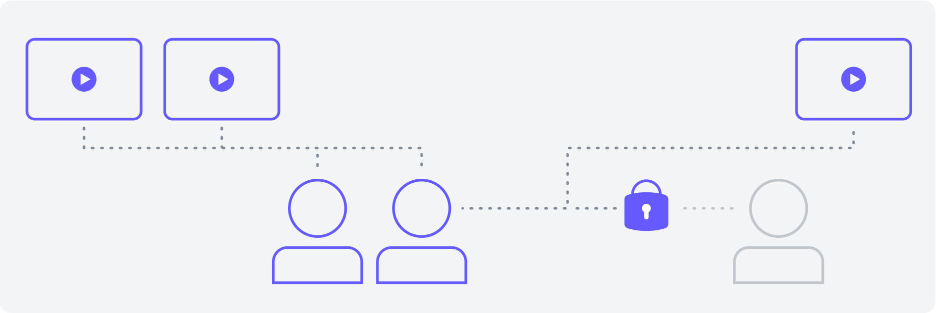
2.0 Determine your needs

2.1 User needs: Evolving with your business

Visual context is inherently useful, which has led to the generation of video workflows in nearly every industry. Video use is no longer limited to reactive use by just security or IT. Professionals across the organization are using video in their day-to-day work. So when considering which camera system is the right fit for your organization, you should evaluate how your organization uses cameras today and how they will use cameras in the near future. The camera system you select should take their needs into account.

When considering which camera system is right for your organization, you should evaluate how you use cameras today and how you will use cameras in the future.





2.1.1 Spread: Who needs camera access?

To decide which camera system is the best fit for your organization, first understand who needs camera access:

- Who is accessing your video data today?
- Why does each user need access?
- What footage does each user need access to?
- Who else will need access in the near future?
- Do users need to collaborate with each other or with external stakeholders?

You may find that camera access will need to extend beyond IT into organizations like HR and operations. While IT may review footage for compliance and incident resolution, operations may review footage to ensure that business processes are running efficiently. Once you have an understanding of who needs camera access, you'll need to make sure your next system has the required features to support each of them.

Key Takeaways

In an organization with a broad-based use of video footage, key features to look out for include:

- Features that support each individual's workflows, such as:
  - Ability to easily view live footage across multiple cameras
  - Ability to easily find and share footage
- Easy collaboration system that allows internal users to annotate and comment on video, and to share it securely with external stakeholders who don't have daily access to the system
- Role-based access control to easily provision users and specify access to the right cameras and features that are relevant to that user

2.1.2 Location: Is viewing primarily local, remote, or both?

Next, understand whether users need to access local cameras, remote cameras, or both:

- Where are users physically located?
- What specific sites does each user need access to?
- Do any users need mobile access?
- What parties do users need to share footage with? Where are they located?

Key Takeaways

Most companies will have users who require remote access. As work and people become more geographically distributed, they require systems that will support that distribution. And you should plan for this distribution to continue to increase by selecting a system that offers:

- Easy remote access, ideally from anywhere in the world
- Mobile access to footage so users can view it from their personal devices when they are on the move
- Unified dashboard that displays camera feeds across locations on one pane of glass

2.1.3 Frequency: How often do they use video?

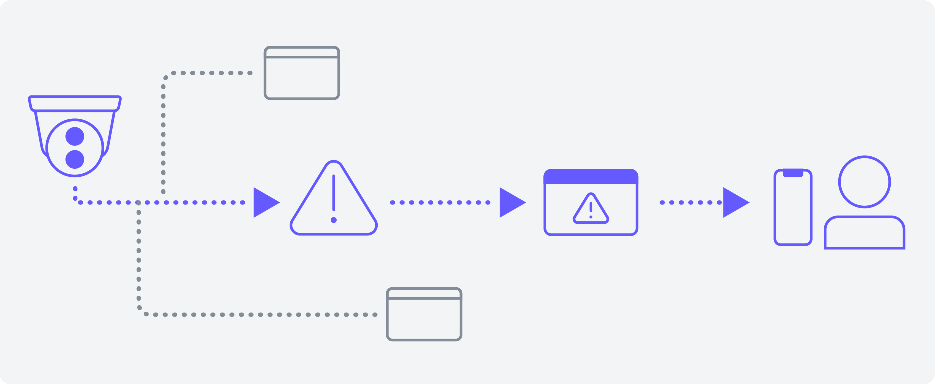
Next, consider how often users access the system:

- On average, how many hours per week does each user spend in the system?
- On average, how many times per week does the user access the system?
- What are the specific tasks they are completing in the system and about how long does each task generally take?
- What other work could each user get to if they didn't have to spend as much time in the system?

Key Takeaways

When this analysis is complete, you might find that your camera system is being accessed more than you had expected, and that other important work is being put on the back burner because it takes users longer than they would like to complete their tasks in the system. If this is the case, it's best to select a system that:

- Significantly cuts down the time it takes to perform each task: The faster a user can find and share footage, the better



2.1.4 Urgency: How time critical are these use cases?

You should also evaluate how time critical the use cases for each user are:

- Can each workflow wait to be executed after something has occurred, or does it need to be executed in real time to be valuable?
- How long after an incident has begun to occur does the user have before they have to act?
- Would proactive measures reduce or even eliminate the time criticality of incidents?

Key Takeaways

In practically every case, there is tremendous value in instant response to incidents to minimize the adverse effects. For example, it’s much better to stop a thief before they leave the premises. And for a manufacturing company, it’s much better to identify a point of failure as soon as the manufacturing line goes down.

The better a system is at allowing users to detect incidents instantly, the more valuable it is. You should look for a system that:

- Allows users to execute their workflows fast enough for them to be valuable
- Allows users to get alerts tailored to incidents that they are looking for

2.1.5 Retention: How much footage needs to be stored?

It's essential for businesses to carefully consider their unique needs and legal obligations when determining the appropriate video retention period for their camera systems. Questions to consider include:

- When viewing footage, how far back historically do users need to go to support their workflows?
- What resolution does the video need to be stored at?
- Do you need continuous or motion-only storage?
- Is redundant storage necessary?
- Is there any footage that must be stored in perpetuity?
- Are there legal or compliance storage requirements that you must adhere to?
- Are your storage needs likely to change in the future?

Key Takeaways

Based on the duration and variability of storage requirements, architectures will compare differently in their built-in ability to store video and their flexibility to accommodate evolving storage requirements.

	NVR/DVR	Cloud Camera	Cloud VMS	AI Camera Systems
Built-in Storage	Usually 14 to 30 days of local storage.	Usually 15 to 365 days of local storage.	Usually 30 to 365 days of local storage.	Usually 30 to 365 days of local storage.
Options of Extending Storage (Local and Cloud)	Some NVRs support installation of additional HDDs. Some offer cloud storage, with additional software setup.	Vendors offer native cloud archiving (indefinitely) and 24/7 retention (usually up to 1 year).	Vendors offer native cloud archiving (indefinitely) and 24/7 retention (usually up to 1 year).	Vendors offer native cloud archiving (indefinitely) and 24/7 retention (usually up to 1 year).
Options for Redundant Storage	Saving locally to a Network Attached Storage (NAS), with additional hardware and software.	Cloud Backup is the only option for redundancy.	Some vendors natively offer RAID storage or saving locally to a NAS.	Some vendors natively offer RAID storage or saving locally to a NAS.
Other Considerations	Storage priced by hard drive volume. Retention period computed based on resolution of storage.	Storage priced by "days of retention." Resolution of stored video varies by vendor.	Storage priced by hard drive volume. Retention period computed based on resolution of storage.	Storage priced by "days of retention." Resolution of stored video varies by vendor.

Figure H: Comparison of storage options offered by different camera system architectures

An important part of selecting the right camera system is selecting the right cameras.

2.2 Cameras: Cutting through the noise

An important part of selecting the right camera system is selecting the right cameras. There are a variety of camera types to choose from. The cameras you need can vary based on specific location and use case. It's common to have different camera types in the same vicinity. Make sure to choose cameras that have sufficient:

- Resolution
- Scene capture
- Range of motion
- Wide Dynamic Range
- Infrared and Night Vision
- Zoom functionality
- Durability
- Ease of installation

Camera resolution options can vary from 2MP to 5MP to 4K, 4K being the highest resolution:

- 2MP resolution is known as "full HD" and is suitable for general surveillance applications and provides clear images for most scenarios
- 5MP cameras are commonly used in commercial and business environments where high-quality video footage is required
- 4K cameras are capable of capturing intricate details and are often used in high-end security systems and advanced video surveillance setups

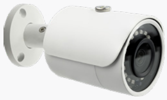
Type	Pros	Cons
Dome	- Discreet design - Nonobvious viewing angle - Vandal-resistant casing - Infrared and night vision	- Limited range of motion - Difficult to adjust once installed
Bullet	- Long-range viewing available in models that have varifocal lenses - High durability, suitable for outdoor use - Ease of Install, flexible mounting options - Highly visible, ideal for deterrence	- Limited range of motion - Visible lens can be tampered with
Turret	- Long-range viewing available in models that have varifocal lenses - High durability, suitable for outdoor use - Ease of install, flexible mounting options	- Difficult to adjust once installed - Shorter range compared to certain bullet camera models
Fisheye	- 360-degree panoramic view, eliminating blindspots	- Distorted edges due to wide-angle lens - Requires dewarping software for proper viewing
Pan, Tilt, Zoom (PTZ)	- Ability to move the camera and zoom in - Ability to track moving objects - Remote control	- Relatively high cost - Mechanical parts can wear out over time
WiFi	- Easy installation without the need for cables - Remote access and control via smartphones and tablets	- Vulnerable to signal interference and network congestion - Limited range compared to wired cameras - Lower reliability in areas with poor WiFi coverage
License Plate Recognition (LPR) 	- High-resolution imaging for accurate plate reading - Integration with databases and access control systems	- Relatively high cost - Limited use beyond license plate recognition tasks - Requires proper positioning and lighting for accurate readings

Figure I: Comparison of different camera form factors

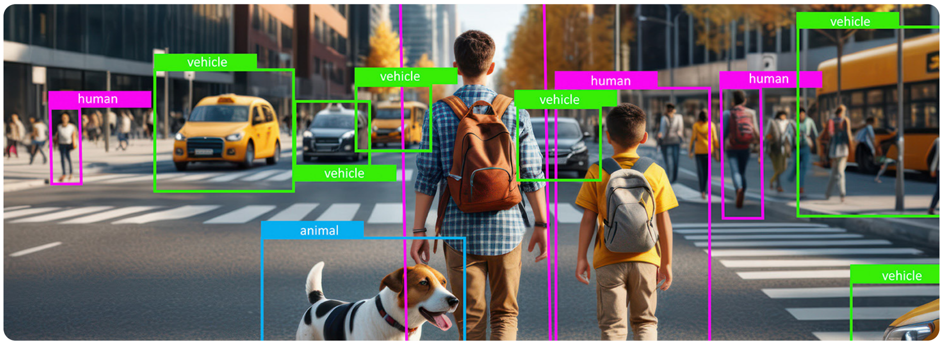
2.3 Software: Evaluating AI options

As innovation in AI is accelerating, more vendors that sell IP cameras and Cloud Cameras or Cloud NVRs are attempting to retrofit AI into their products. Many vendors may seem to have similar products. In this landscape, it's useful to understand the differences underneath the marketing so you can decide which vendors align most with the needs of your users—and figure out what's the best fit for your needs.

AI offerings on the market can be tiered based on the underlying AI technology they leverage.

Tier 1: Motion, people, vehicle detection

The first tier of AI offerings includes motion, people, and vehicle detection. These features have become common across modern systems and provide a base level of AI-driven value.



It's useful to understand the differences underneath the marketing so you can decide which vendors align most with the needs of your users.

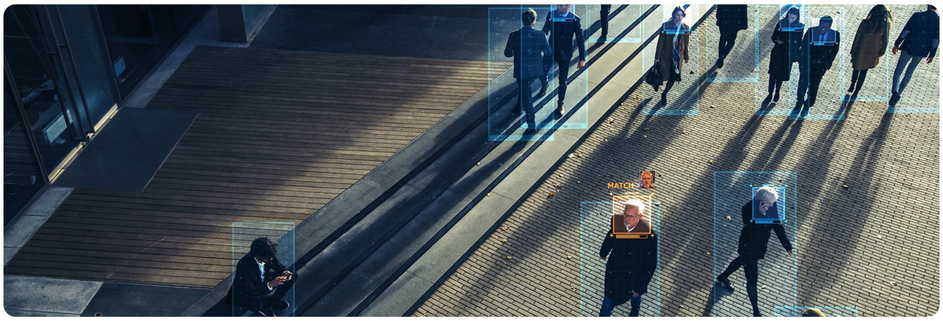
Motion detection cameras can trigger recordings or alerts when any movement is detected within a monitored area. While this feature is useful in tracking unexpected activity in an area during off hours, it is missing the context of *what* is in motion.

People detection takes this a step further, enabling the camera to distinguish human presence. This feature facilitates automated alerts when a person is recognized in the scene. This could be useful, for example, in retail environments to monitor the number of customers that visit a location, or in a common work environment to identify when the first person arrives to work.

Vehicle detection allows AI cameras to identify and differentiate vehicular presence, which is useful in applications like counting the number of vehicles that are in a parking lot to monitor occupancy levels, or alerting loading bay workers when a delivery truck arrives.

Tier 2: Facial recognition, license plate recognition

The second tier includes features such as facial recognition and license plate recognition. These features can cover more advanced use cases that drive faster processing and improved business value and safety.

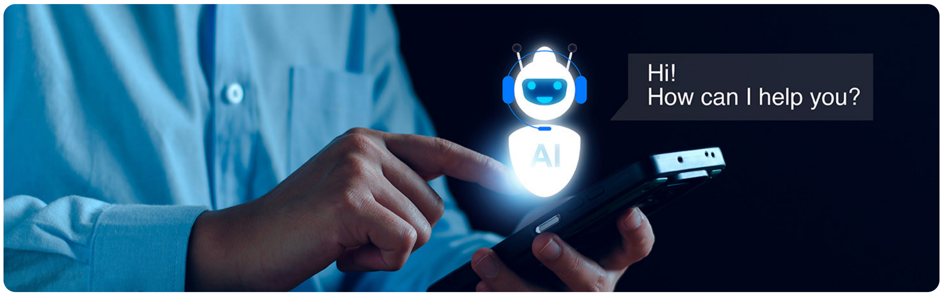


Facial recognition can apply in various use cases across industries. For example, a retail store could enable tailored customer experiences by identifying frequent shoppers and offering personalized recommendations or discounts, fostering customer loyalty. In law enforcement and public safety, it could be used to aid in locating missing persons or identifying suspects by cross-referencing facial data with criminal databases or prior video footage.

License plate recognition could be applied in transportation and parking management. For instance, it could facilitate automatic toll collection on highways, or optimize parking facilities by automating entry and exit processes. Additionally, in auto services this technology could be applied to quickly process damage claims by locating relevant footage by simply inputting a license plate number.

Tier 3: AI assistants, universal search, action detection

The third tier has capabilities that leverage foundation models. As a result, this tier offers advanced features that unlock new use cases that significantly expand the business value of video.



AI assistants can automatically index a physical environment, categorize the objects and concepts in the scene, and provide intelligent prompts and contextual alerts to improve business safety and efficiency. For example, an AI assistant at a retail store could prompt the user to move a popular item that drives the most foot traffic to the back of the space in order to increase spontaneous purchasing, similar to how Costco

strategically places their popular rotisserie chicken in the back of all their locations to boost overall revenue. Or, as another example, users could get a notification automatically when someone is in a restricted zone or not following safety protocol on the manufacturing floor, so they could take action before anything goes wrong.

Universal search allows users to run a search across all cameras for specific custom objects or concepts, and adaptive search allows users to tailor search results and adapt them to their preferences. These functionalities enable quick and precise data retrieval. For instance, investigators could swiftly search through extensive video archives for specific events such as break-ins, suspicious activities, or specific individuals entering or leaving a location, aiding in criminal investigations. Businesses can utilize this feature to search for customer interactions, track inventory movements, or identify operational inefficiencies, allowing for detailed analysis and data-driven decision-making.

Action detection (pose and speed) allows users the ability to understand how people or objects are positioned and the speed at which they are moving. For example, pose detection could be used in a workplace setting to alert medical resources if someone is having a seizure, or at a school if children begin to fight. And speed detection can alert manufacturing management if an employee is driving a forklift too quickly, or if their manufacturing line is moving too slowly.

Connecting your needs to AI capabilities

Once you've decided the level of AI capabilities you need to procure to meet your organization's needs, there are key considerations to evaluate if a particular solution is the right fit.

	Few Users (1–5)	**Many Users** (5+)
Few Locations (1–3)	• Limited video workflows • Tier 1 AI is likely to meet your needs	• Moderate video workflows • Tier 2 AI is likely to meet your needs
Many Locations (3+)	• Moderate video workflows • Tier 2 AI is likely to meet your needs	• Heavy video workflows • Tier 3 AI is likely to have significant ROI in terms of time saving and business value created

Figure J: Mapping tiers of AI capabilities to organizational needs based on extent of video workflows

Evaluating AI Offerings

All AI products are not created equally. The most important underlying difference that affects the long-term AI strategy is the choice of architecture of the system. Products from each of the eras (IP cameras, Cloud, AI Camera Systems) incorporate different hardware and software architectures to enable AI in their products. This affects the capabilities that organizations get today and affects the ability for the product to keep up with the rapidly changing AI landscape.

	IP Cameras	Cloud Camera	Cloud VMS	AI Camera Systems
Hardware to Support AI	**Edge-only:** No AI-specific microchips on hardware. Simple AI models run on existing processing capability of camera/NVR.	**Cloud-only:** AI-specific microchips on some hardware. Video uploaded to the cloud for AI inferences.	**Cloud-only:** No AI-specific microchips on hardware. Video uploaded to the cloud for AI inferences.	**Hybrid:** Purpose-built with microchips to run AI models at the edge as well as in the cloud.
Level of AI Capabilities	Usually Tier 1	Usually Tier 2	Usually Tier 2	Tier 3 capabilities out of the box
Headroom of Future Improvement	**Limited:** No AI-specific hardware limits use of additional more powerful models.	**Impractical:** AI-specific microchips have limited power budget and performance. Video can be uploaded to the cloud for inferences, which would be expensive for the same level of performance.	**Impractical:** AI-specific microchips have limited power budget and performance. Video can be uploaded to the cloud for inferences, which would be expensive for the same level of performance.	**Large:** Hybrid AI architecture leverages the best of the edge and cloud to create performance headroom, and allows for easy ongoing addition of improved models.

Figure K: Comparison of different AI capabilities supported by different camera system architectures

Once you've decided the level of AI capabilities you need to procure to meet your organization's needs, there are key considerations to evaluate if a particular solution is the right fit. It is important to evaluate if the product can deliver in practice the value that it promises on paper. Key questions to keep in mind are:

Usability

- Does the product deliver AI at a level of performance (accuracy and latency) to solve your users' problems exactly when they need it solved?
- Is the product easy to use for any user in your organization, or will it require training before your organization is able to see value from it?

Interoperability

- Does the product work with your existing cameras and networks?
- Is the product compatible with the clients' devices that your users execute with?

Scalability

- Is it easy to add more locations, cameras, and users to allow the product to scale into your organization?
- Can the product easily add more advanced AI models over time so that your business has the latest and greatest through the life of the system?

Cybersecurity

- Does the product natively encrypt video at-rest and in-transit?
- Does the product provide you with the ability to easily provision and monitor user access?

Because of the differences in underlying technologies, all AI products are not created equally. It is important to evaluate if the product can deliver in practice the value that it promises on paper.

2.4 Cybersecurity: Market standards in 2023

Why is cybersecurity important?

The internet is a vast and interconnected network, making it susceptible to a wide range of threats. As all software moves into browser tabs, the need to protect your personally identifiable information[1] (PII) from unauthorized access, breaches, and misuse becomes more critical than ever.

Your information is most vulnerable when it is transmitted across the internet. A data breach or security risk can expose PII to unauthorized individuals and be especially damaging to company reputation.

Because workers are becoming increasingly geographically distributed, remote camera access has become a table stakes feature. The challenge in the video surveillance industry is that most cameras are not secure, in fact, nearly all cameras stream unencrypted traffic natively. And connecting those cameras to the cloud is **even more dangerous**[2]. This shift highlights the need to protect PII, and even more critically, biometric information. After all, these systems are observing every detail about your crucial physical assets: your people, your customers, your equipment, your products, your services, and more. This makes video your most valuable data asset.

In fact, the camera brands that are the most economical for customers, and the most dominant in the marketplace, are getting **increasingly banned**[3] by the US government due to backdoors and exploits that enable other nation states to access the footage.

[1] The U.S. Department of Labor defines PII as "information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."

[2] **Insecam - Live cameras directory**

[3] Dagostino Electronic Services: **'FCC to Ban Hikvision, Dahua Cameras, in all USA Facilities'**

As an example, customers who wish to receive federal funding must adhere to NDAA compliance and therefore purchase their video surveillance equipment through an approved list of manufacturers.

A zero-trust or identity-based model is critical to a secure video surveillance system

In the context of surveillance systems, a zero-trust or identity-based model refers to an approach where trust is never assumed, even within a trusted network environment.

> Zero-trust refers to an approach where trust is never assumed, even within a trusted network environment.

Traditional security models often operate on the premise that everything within the network perimeter is trustworthy. However, a zero-trust model challenges this notion, asserting that trust must be continuously verified, regardless of whether the user or system is inside or outside the network perimeter. This means that every user, device, or application trying to access the system, regardless of their location, is treated as a potential security threat.

Access permissions are granted on a need-to-know basis and are dynamically adjusted based on various factors, including user identity, device security posture, and behavior patterns. By adopting a zero-trust model, organizations can significantly enhance the security of their video surveillance systems, ensuring that sensitive video data remains protected from unauthorized access, breaches, and other security risks.

For any surveillance system, it is highly recommended that you select a zero-trust model to best protect your data. Best-in-class systems do not compromise security and also implement:

Encryption

- **Data in Transit:** Video is encrypted before being transmitted over networks. This ensures that even if intercepted, the data is unreadable to unauthorized individuals
- **Data at Rest:** Stored video is encrypted to protect it from physical theft or unauthorized access to databases or storage devices

Access Control

- **Role-Based Access Control (RBAC):** Access control policies that grant access to video data and particular features based on job roles and responsibilities
- **Audit Logging:** The most secure RBAC systems include audit and logging features to track and record access activities. This helps in monitoring and detecting security breaches and compliance with security policies

SSO/SAML Integration

Centralized control over authentication and authorization improves security by allowing administrators to implement stronger authentication methods and enforce access policies consistently across multiple software services, while also allowing for a smoother user experience. This also simplifies on-boarding and off-boarding of employees.

Rotating/Expiring Tokens and Keys

Rotating tokens and keys reduces the window of vulnerability. If an attacker gains access to a token or key, they have a limited time to misuse it before it becomes invalid. This shortens the time during which the attacker can exploit the compromised credentials

3.0 Compare your options

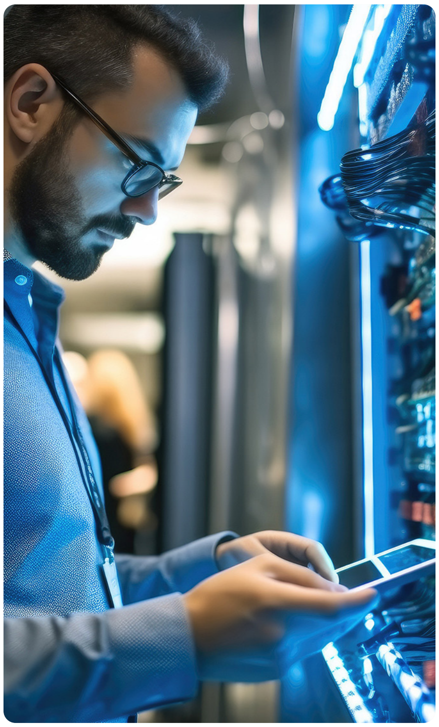
3.1 Understand implications for IT

As security cameras have proliferated in the workplace, managing security systems has transitioned from being a one-time set-and-forget for IT to an ongoing commitment. IT professionals are bogged down with requests to retrieve video and root causing system downtime across a patchwork of systems across locations. And as the need to access and retrieve video increases in frequency, these demands on IT are only intensifying. This is making the choice of the right camera system even more critical.

Managing security systems has transitioned from being a one-time set-and-forget for IT to an ongoing commitment.

Considerations as you think through your next system

- **Meet the minimum requirements of a modern system:** Cloud is table stakes in video surveillance today. This encompasses easy remote viewing across locations, easy search and collaboration, and best-in-class cybersecurity. Most organizations maintain their video surveillance systems for three to five years. If your users don't need this today, they may need this sooner than your next refresh cycle.



- **Evaluate feature velocity of the vendors you want to partner with**: The current pace of AI development is unprecedented. New products launch weekly. This means that a product that has unique features today may not be as unique in the near future. When selecting your next system, it's important to select a system that has a proven track record of high feature velocity, so you can trust that the product will continue to keep up with the rapid pace of AI development. This will allow your users to benefit from new features more quickly, which will be a compounding advantage over the life of the system. Your camera system can become an appreciating asset rather than a cost center.

- **Proactively evaluate the health of your networks:** As users pull for more video, the utilization of your networks may rise. In that case, you may run into bandwidth constraints if your system of choice of bandwidth consumptive. Your data is also at risk of being exposed to malicious actors if not properly protected.. To evaluate the health of your networks, ask questions like:

  - Do we have sufficient bandwidth for our video workflows today?

  - Are there unexpected data flows or unusually high bandwidth consumption observed in the surveillance system traffic?

  - How often do unauthorized devices attempt to access the network?

- **Make sure you have the observability to easily manage your systems across locations:** As your organization grows, managing the network and connected devices becomes more and more complex. Observability into network health is a crucial aspect of network management and monitoring. Best-in-class video surveillance systems can provide insights into the health of the surveillance system's components, such as cameras, recorders, and network infrastructure. This information helps in planning maintenance and replacing or upgrading components as needed to avoid unexpected failures. Surveillance cameras may encounter issues like lens obstructions, misalignment, or electrical problems. Observability can help in monitoring the health of individual cameras, ensuring they are functioning correctly. Additionally, user management is a critical component of IT and information security, particularly in organizations that rely on digital systems and networks. This ensures easy provisioning and modification of access for employees, contractors, and other users.

3.2 Find hidden costs

	Cloud Cameras	Cloud NVR	AI Camera System
Cameras	Requires purchase of proprietary cameras.	Most vendors are agnostic to IP cameras using RTSP/ONVIF protocols.	Most vendors are agnostic to IP cameras using RTSP/ONVIF protocols.
TCO implications: Immediate and future camera replacements baked into the choice of system.			
Local Storage	On-board flash memory storage is expensive relative to HDD-based storage. At higher camera counts, TCO will surpass a cloud NVR-based solution.	Local storage on HDDs is cost-effective. This is likely to be more cost-effective at higher camera counts.	Local storage on HDDs is cost-effective. This is likely to be more cost-effective at higher camera counts.
TCO implications: Relative costs of storage, especially at higher camera counts.			
Software	Easy-to-use software, usually no training required.	Unintuitive user interface that might require additional training and ongoing support from IT.	Easy-to-use software, usually no training required.
TCO implications: Resources required for end-user adoption. Products that are difficult to use are likely to require initial and ongoing IT support.			
AI Capabilities	Usually Tier 1, but in some cases Tier 2.	Usually Tier 1, but in some cases Tier 2.	Tier 1, 2 and 3 AI capabilities out of the box. Hybrid AI enables features to be more powerful, more useful, and more responsive.
TCO implications: Cost of ongoing upgrades to keep up with the latest and greatest in AI over the life of the system.			
Network/ Bandwidth	Customers in limited bandwidth areas are likely to need to upgrade network infrastructure to support video consumption requirements	Customers in limited bandwidth areas may not need to upgrade network infrastructure to support video consumption requirements as long as they're not looking for Tier 3 AI use cases.	Customers in limited bandwidth areas may not need to upgrade network infrastructure to support video consumption requirements even for advanced AI use cases.
TCO implications: Network/SD-WAN upgrades required to deliver desired user experience and functionality.			
Installation	All cameras need to be replaced. Easy setup once new cameras are mounted.	Cameras may not need replacements but NVR installation will require access to the local network.	Cameras may not need replacements but IVR installation will require access to the local network.
TCO implications: Total cost of setup including installation of cameras, setup and configuration of equipment.			
Post-Sales Support and Warranty	Defects and issues arise in the best of products and cameras may stop working over the life of the contract. Some vendors offer 10-year warranties on cameras.	Vendors usually offer warranty for the life of the contract. Some vendors don't charge separately for ongoing support	Vendors usually offer warranty for the life of the contract. Some vendors don't charge separately for ongoing support.
TCO implications: Warranty on hardware. Additional cost of support based on vendor/VAR agreements.			

Figure L: Hidden TCO implications of different camera system architectures

3.3 Checklist: Cover all your bases

□ Know your options

- □ **DVR/NVR: Proprietary cameras, local storage, limited remote access, limited AI, cybersecurity add-on**
- □ **Cloud**
  - □ Cloud cameras: Proprietary cameras, cloud storage, remote access, cloud-only AI, native cybersecurity
  - □ Cloud NVR: Camera-agnostic, cloud storage, remote access, cloud-only AI, native gold standard cybersecurity
- □ **AI Camera Systems: Camera-agnostic, cloud storage, remote access, hybrid AI, native gold standard cybersecurity**

□ Understand your users' needs

- □ **Spread: Who needs access?**
- □ **Location: Local, remote, or both?**
  - □ Do any users need remote access?
  - □ What parties do users need to share footage with?
- □ **Frequency: How often do users use video?**
  - □ On average, how many times per week does the user access the system?
  - □ What are the specific tasks they are completing in the system and about how long does each task generally take?
- □ **Urgency: How time critical are the use cases?**
  - □ How long after an incident has begun to occur does the user have before they have to act?
  - □ Do users need to predict an incident before it occurs?
- □ **Retention: How much footage needs to be stored?**
  - □ When viewing footage, how far back historically do users need to go to support their workflows?
  - □ Is there any footage that must be stored in perpetuity?

□ Know which camera models fit your needs

- □ **Resolution: What resolution will allow your users to complete their workflows?**
- □ **Zoom functionality: Do your cameras need to be able to zoom in?**
- □ **Durability: What conditions will your cameras be in and how long do you need them to last?**

Checklist: Cover all your bases (continued)

□ Understand what tier of AI, if any, is right for you

- □ **Tier 1: Common AI offerings**
  - □ Motion: Detect when something moves
  - □ People and Vehicles: Detect when a person/vehicle is present
- □ **Tier 2: More advanced capabilities that drive faster processing and improved business value**
  - □ Facial Recognition: Monitor specific individuals on the premises
  - □ License Plate Recognition: Automatically track license plate numbers
- □ **Tier 3: Unlock business value through workflows not previously possible**
  - □ AI Assistants and Universal Search: Automatically index the physical environment, search for custom concepts across all cameras, provide useful prompts
  - □ Action Detection: Understand how objects and positioned and at what speed they are moving

□ Measure yourself against the cybersecurity gold standard: Zero-trust

- □ **Encryption: Data is unreadable to unauthorized individuals**
- □ **Access control: Only authorized users have access**
- □ **SSO/SAML Integration: Centralized control over authentication and authorization**
- □ **Rotating/Expiring Tokens and Keys: Shorten window of vulnerability**

□ Understand hidden costs that contribute to your Total Cost of Ownership

- □ **How much will you need to spend on cameras immediately and in the medium term?**
- □ **How much time will it take to train users to effectively use the software?**
- □ **Are you paying separately for upgrades to AI capabilities?**
- □ **To install the system, will you be required to upgrade your network?**
- □ **Is support and customer success included?**
- □ **If hardware fails, what is the cost of replacement hardware?**

□ Make a choice that sets IT up for success

- □ **Meet the minimum requirements of a modern cloud system**
- □ **Evaluate the feature velocity of the vendors you want to partner with to benefit from future developments in AI**
- □ **Proactively evaluate the health of your networks to support your video workflows**
- □ **Make sure you have the observability to easily manage your system across locations**

About Spot AI

Spot AI is the industry leader in AI Camera Systems, on a mission to create a safer and smarter physical world with the power of Video Intelligence. Spot AI's Camera System equips organizations with video-driven insights that helps any user in any business instantly surface and resolve problems. Spot AI is deployed at thousands of locations across the U.S. and trusted by leaders across 17 different industries.

Trusted by industry leaders

HALLIBURTON | WINE DIRECT | Leggett & Platt | Goodwill of Western New York | Ken Garff (WE HEAR YOU) | Endeavor Energy Resources

RAHR | Glide XPRESS | SCHEELS | BARRY'S | MOAB REGIONAL HOSPITAL | Emirates dnata THE EMIRATES GROUP

CULLMAN COUNTY SCHOOLS EXCEPTIONAL EDUCATIONAL EXPERIENCES FOR EVERYONE EVERY DAY | LPS | Athens Area School District | CAMBRIDGE Maryland | SHA Sylacauga Housing Authority Since 1943 | School District of Neillsville

Rated #1 in physical security

- Momentum Leader FALL 2023
- Users Most Likely To Recommend FALL 2023
- Best Support FALL 2023
- Easiest To Do Business With Mid-Market FALL 2023
- Easiest Admin Mid-Market FALL 2023
- Easiest Admin FALL 2023
- Best Meets Requirements FALL 2023
- Mid-Market High Performer Americas FALL 2023
- High Performer Americas FALL 2023
- High Performer Mid-Market FALL 2023
- High Performer FALL 2023 — Physical Security
- High Performer FALL 2023 — Video Surveillance

Stay tuned

For more information, visit **www.spot.ai** or email **sales@spotai.co**.

spot.ai

Forbes THE Cloud 100 RISING STAR

IA 40 winner

Spot AI builds an easy-to-use camera system that enables effortless Video Intelligence for every business. For more information, visit www.spot.ai.