

Physical security shift happens

---

# IT Guide to a modern physical security infrastructure

*Taking a sane and staged approach to a modern future*



## EXECUTIVE SUMMARY

# Physical security shift: Navigating modern solutions

The physical security industry is undergoing a monumental shift, driven by advancements like cloud computing and artificial intelligence (AI). These innovations are re-shaping the way we safeguard and protect people, places, and assets.

While the industry is in the midst of a revolution, for businesses, it's more of an evolution to a modern future. Despite the enormous promise of these new technologies, finding the right physical security partner to navigate this journey can be challenging. It's easy to become captivated by flashy features and end up spending a fortune for a solution requiring a complete system overhaul. However, a staged approach often works best, allowing for a gradual evolution and customizations that meet your needs on your timeline.

Upgrading your physical security infrastructure is a journey that is easier when you understand your business needs, the solutions available, deployment choices, and purchasing options. This guide aims to help businesses intelligently navigate the physical security landscape. Our goal is to leave you better equipped to modernize your physical security infrastructure in a sane, staged, and scalable way.



**Steve Prodger**  
CRO, Arcules

## The future is in the clouds



### Using Cloud

Businesses are already using a cloud-based video surveillance solution.\*



### Migrating to cloud

Businesses are planning to migrate to cloud-based video surveillance in the next two years.\*



### Leveraging AI

Businesses using cloud-based video surveillance are leveraging AI for enhanced functionalities like behavioral analysis.\*

# Table of contents:

## Executive Summary

---

Physical security shift: Navigating modern solutions 01

## Your Journey to Cloud

---

Chapter 01 Understanding the new video surveillance landscape 03

Chapter 02 Defining your business needs 05

Chapter 03 Evaluating your deployment options 08

Chapter 04 Open vs. closed infrastructure 10

Chapter 05 Busting common cloud myths 11

Chapter 06 Cutting through the AI hype 13

## Conclusion

---

Maximizing the value of your investment 15

## CHAPTER 1

# Understanding the new video surveillance landscape

Modernizing your physical security infrastructure begins with better understanding the overall landscape, which includes a mix of traditional players and tech-focused upstarts. To choose the right solution for your business, it's crucial to know the key players and what their relative agendas may be. Let's explore the key categories of companies in this space, starting with video surveillance, arguably the most critical component of your physical security infrastructure:



## Video surveillance

---

### Cloud native video surveillance software providers

These companies offer video surveillance solutions that are designed to operate entirely in the cloud, providing scalable and flexible storage, video analytics, and remote access control capabilities without the need for on-premise infrastructure.

### All in one video surveillance + hardware providers

These providers deliver integrated systems that include both hardware (cameras, DVRs/NVRs) and proprietary software, creating a closed ecosystem where all components are designed to work seamlessly together.

### On-premise only providers

Specializing in solutions that are exclusively deployed on-site, these companies require local servers and storage. This can offer higher security and control but less flexibility compared to cloud-based solutions.

### Hybrid on-premise/cloud providers

These providers offer versatile solutions that can be deployed as a combination of on-premises and cloud services, allowing for benefits such as AI-enhanced video analytics and scalable storage options. Hybrid deployment options are being offered by vendors that started out as on-premises solutions and those that are cloud native, with the goal of helping businesses transition to a more modern infrastructure.



## Other Critical Security Infrastructure

---

### Access control solutions

These companies provide systems that manage and control entry to buildings or specific areas, often integrating with other security systems to enhance overall security through keycards, biometrics, and mobile credentials. When integrated with video surveillance solutions, they provide greater situational awareness for end users.

### Alarm monitoring solutions

These solutions focus on detecting and alerting for security breaches such as intrusion, fire and gas leaks, and other emergencies. They are often integrated with various sensors and communication systems to provide real-time monitoring and response capabilities.

### Lighting and visibility

Darkness is a criminal's best friend. When your business, parking lot, and other areas are poorly lit, it is more likely to mark your establishment as a target. Upgrading your lighting in and around your business can deter criminal activity making your business seem more secure and even inviting to potential customers.



## Hardware providers

---

### Hardware / camera / device (IoT) manufacturers

These manufacturers design and produce the physical devices used in security systems, such as cameras, sensors, speakers, intercoms and other IoT devices, which are essential for capturing and transmitting surveillance data.



## Channel Partners

---

**System integrators:** These companies specialize in combining various security products and systems from different vendors into a cohesive solution tailored to the specific needs of a client, ensuring seamless operation and interoperability.

**Distributors:** These entities act as intermediaries, purchasing security products from manufacturers and selling them to end-users, resellers, or system integrators, often providing additional services like technical support and training.

## CHAPTER 2

# Defining your business needs

Before jumping into a big video surveillance system upgrade, it's important to define your business needs. You'll want to evaluate your overarching goals for the project, who owns the decision and needs to be involved, what if any limitations exist such as bandwidth, how much budget you have, and what outcomes you are looking to achieve.

### Questions to guide the process:

In order to fully understand your needs, consider asking yourself a series of key questions before beginning the evaluation process. These questions are designed to elicit exactly what kind of system and requirements are necessary to get your business where it needs to be based on your current infrastructure, and ultimately choose a partner that will help you move to a more modern environment that fits your business.

## What are your primary objectives and outcomes?

Define your overarching goals and outcomes. Goals can vary from simple reactive video monitoring to theft prevention for a retailer or protecting the lives of students, faculty, and staff for a school. Outcomes can range from improved operational efficiency, i.e. less time viewing videos and more proactive response to incidents, to more secure infrastructure.

## What are the areas to be monitored?

Consider how many sites you have and if you need surveillance both indoor and outdoor or a mix of both. Create site maps and/or floor plans and consider what you need to deter, detect, delay and defend your business - visibility, lighting, cameras, horns, intercom, sensors, access control, etc.

## What unique use cases will require specific cameras?

Identify high traffic areas, access points, and other points of interest that might need special attention (i.e. a loading/delivery zone, mailing room). Think through any special cameras needed based on specific business needs - e.g. pan-tilt-zoom (PTZ) or wide angle for better visibility of an area, a drone camera for campus perimeter scans, body worn cameras for employees, thermal cameras for temperature scans, etc.

## What cameras can you reuse?

Take inventory of all your existing cameras and consider reusing newer cameras to minimize upfront costs. Keep in mind, if the camera footage from older cameras is captured in the cloud with the right video management system, additional analytics can be applied, effectively giving old cameras an upgrade.

## **What is your cloud modernization strategy?**

Choosing a system that integrates with your overall IT infrastructure and cloud strategy is critical for ease-of-use and integrations across the organization. Make sure that any vendor you choose is consistent with your overall cloud and modernization strategy.

## **What critical infrastructure integrations are needed?**

Consider other critical security infrastructure and any needs for integration. Keep in mind that integrating your devices creates better overall situational awareness. Create a checklist of all your security functions and solutions to help you choose the right solutions.

## **What are your storage requirements?**

Understanding how long you need to keep video footage and how secure that footage needs to be will help you select the right deployment and storage options for your business.

## **Do you need remote access?**

Enabling remote access to critical video surveillance footage and data is often a key requirement for organizations with centralized IT management covering multiple locations, and not all solutions offer this functionality.

## **What are your maintenance and cost requirements?**

There can be wide disparities between different types of systems when it comes to ongoing cost-of-ownership, and it's important to thoroughly understand how each vendor you're considering approaches maintenance and additional costs.

## **Have you defined your customer support needs?**

Your relationship with your video surveillance vendor shouldn't end once you're signed a contract and installed a system, and it's critical to choose a partner who is dedicated to providing a superior customer experience, along with a product that is always evolving to help you get the most out of your purchase.

## **What industry standards must you comply with?**

It is critical that any service you choose contains stringent data protection that complies with critical standards and regulations— especially those in highly sensitive industries like healthcare, data storage, or education.

## **What additional use cases can help your business?**

Consider other potential use cases for video data that might help you operate more efficiently. For example, in healthcare you might want to leverage video to help reduce wait times. For a retail business it might help to gather data around high-traffic areas or end cap displays for advertising purposes.



## CHAPTER 3

# Evaluating your deployment options

Choosing a video surveillance solution isn't just about pure cloud vs. on-premise - other deployment options exist including a hybrid or mix-and-match approach. Let's explore the benefits and limitations of each.



### Pure Cloud

Fully cloud-based solution utilizing cloud infrastructure for storage, processing and management of video data.

#### Benefits:

Data storage scalability, accessibility, advanced analytics, reduced IT maintenance.

#### Limitations:

High bandwidth requirements, potential latency, data privacy concerns.



### Edge

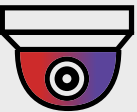
Video data processed and stored locally on an edge device.

#### Benefits:

Reduced bandwidth, real-time analysis, centralized cloud control.

#### Limitations:

Limited storage, dependence on edge device capability.



### Camera to Cloud

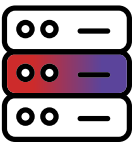
Video data processed and stored locally on the camera and streamed to the cloud.

#### Benefits:

Reduced bandwidth, real-time analysis, simplified infrastructure.

#### Limitations:

Potential latency, data privacy concerns with on camera storage (tampering or damage to camera), requires data backup strategy.



### On-Premises

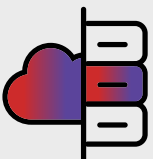
Data stored, processed, and managed on local servers.

#### Benefits:

Complete control over data, compliance with strict regulations.

#### Limitations:

High upfront hardware costs, ongoing maintenance.



### Hybrid

Combines cloud and on-premise systems for flexibility.

#### Benefits:

Balance of control, cost, and performance, scalable storage and analytics.

#### Limitations:

Complexity of managing hybrid infrastructure.



### Mix and Match

Integrates elements of cloud, on-premise, and hybrid solutions.

#### Benefits:

Customizable to unique needs, adaptable, optimized for specific use cases.

#### Limitations:

Complexity in integration, potential compatibility issues.

## What's the right deployment option for you?

If you are looking to migrate your physical security infrastructure to the cloud, choosing a flexible VMS that supports multiple deployment models ensures adaptability to diverse and changing business requirements and technological advancements.

While one approach may seem like the most ideal option it is important to understand the origin and agenda of the vendor you are working with — did the vendor start as an on-premises solution or are they cloud native? Does the vendor manufacture their own hardware?

Vendors that started out as on-premises tend to have more limited cloud benefits, possibly just storing video in the cloud. Vendors that are all-in-one hardware/software solutions may require rip and replace or have dependencies on hardware they sell. Vendors that started as cloud native may have limited integration hooks into on-premises solutions.

It is also important to consider your ultimate destination — if you are looking to fully migrate to the cloud at some point, going with a cloud native provider that can help you make use of on-prem servers as you phase out the infrastructure may be a more prudent approach.

## CHAPTER 4

# Open or Closed, That is the Question.

In addition to deciding between cloud and on-premise deployment options, you'll need to weigh the advantages of "open" and "closed" solutions.

	Closed solutions	Open solutions
	Vertically integrated systems that work with one brand of cameras and devices, usually manufactured by the same company.	Compatible with devices from multiple manufacturers and can integrate with other critical security infrastructure easily.
<b>Device Choice</b>	Restricted to one brand's cameras and devices.	Freedom to choose cameras and devices from multiple vendors.
<b>Cost</b>	Often higher due to proprietary hardware and subscriptions, and upfront costs to rip and replace existing infrastructure.	More cost-efficient with competitive hardware pricing and ability to reuse existing devices and upgrade as devices age out.
<b>Vendor Lock-In</b>	High, dependent on a single vendor. In some cases devices become bricks if you no longer use the vendor's software.	Low, no dependency on a single provider. These vendors need to work hard to earn your business every day.
<b>Collaboration</b>	Minimal and limited, within the vendor's ecosystem.	An open ecosystem encourages collaboration and innovation among multiple parties.
<b>Long-Term Implications</b>	Less flexible, harder to adapt to new technologies.	More adaptable to evolving technology and business needs.

The choice between an open and a closed solution is not just about the immediate features offered, but rather about the long-term implications and flexibility that each option provides. At the core of this debate lies the principle of openness versus closedness, a fundamental technology question with serious potential ramifications.

## CHAPTER 5

# Busting common cloud myths

A modern approach to physical security often requires shifting away from heavy reliance on on-premises technology to cloud-based solutions. However, businesses are sometimes reluctant to make this transition due to outdated notions or outright falsehoods about the cloud experience. Let's examine some common cloud myths and set the record straight.

### Myth #1:

**Cloud migration is too complex.**

### Truth:

Today's modern cloud solutions offer user-friendly interfaces, automated data transfers, network-ready system checks, and robust security measures. Businesses can also start with a hybrid approach and gradually move to a full cloud deployment.

### Myth #3:

**The ROI on cloud isn't there yet.**

### Truth:

When it comes to cost structure, cloud solutions typically follow a pay-as-you-go pricing model, reducing initial costs. They also require less maintenance since the provider handles system upkeep.

In contrast, on-premise systems may involve substantial upfront costs for hardware and infrastructure as well as demand more hands-on maintenance. Businesses report up to a 30% reduction in total cost of ownership (TCO) compared to traditional on-premises solutions, due to savings on hardware, maintenance, and operational costs.

### Myth #2:

**The cloud is less secure than my data center.**

### Truth:

Cloud providers like Google implement robust security measures such as data encryption, access controls, data redundancy, 24/7 monitoring and more.

On-premises storage provides more control but requires rigorous management of backups, updates, and maintenance, all of which can pose risk if not managed effectively. In fact, in a recent survey around 70% of users reported that the benefits, such as enhanced security features and regular updates provided by cloud service providers, outweighed their initial security concerns.

### Myth #4:

**I need to replace all my infrastructure to move to the cloud.**

### Truth:

While certain "closed" cloud solutions may require businesses to replace existing cameras and hardware in order to work with proprietary systems, open cloud solutions can integrate with your existing cameras and often upgrade their functionality with "smart" features.

**Myth #5:**

**I lose control of my data in the cloud.**

**Truth:**

Businesses do not lose control of their data when using cloud-based solutions. In fact, the customer or business needs to define and manage who has access to the data under what circumstances, ensuring only authorized personnel can access sensitive information.

**Myth #6:**

**A cloud solution does not meet my feature requirements.**

**Truth:**

Cloud solutions are becoming increasingly feature rich and provide additional benefits that on-premise solutions can't match such as remote access to live and recorded security footage, regular product updates, and easy management.

## CHAPTER 6

# Cutting through the AI hype

Artificial Intelligence (AI) plays a crucial role in video surveillance, enabling features such as facial recognition, object detection, and behavioral analysis. A truly effective AI-driven video surveillance solution will offer tangible benefits that actually matter to your day-to-day operations, not simply promises of some ideal future. When evaluating AI capabilities, look for a VMS solution that gives you the following benefits:



### Continuous learning

---

AI learns from data, the more data it is exposed to, the smarter it gets. Cloud systems are inherently exposed to more data across entire businesses, enabling better learning that can be applied back to the business. On-premises systems, with data stored locally and siloed from the organization, can't fully benefit from an AI learning model.



### A view of the complete picture

---

AI-driven video analytics are potentially extremely powerful, but not all vendors are created equal. Look for a solution that analyzes data across all your devices and presents that analysis to you in a single platform and in a clear, usable way.



### Proactive response capability

---

One of the key advantages of AI in a video surveillance solution is the ability to offer proactive capabilities, with real-time incident detection and alerts for immediate response. Ensure the video surveillance solution you're considering offers true proactive capabilities before signing on the dotted line.



### Recognizing the limitations of visual AI

---

The effectiveness of AI algorithms vary. One way to measure the effectiveness of visual AI is through an accuracy rating score, which essentially measures how confident the algorithm is at identifying visual information. While the accuracy scale theoretically goes up to 100%, the very best visual AI implementations on the market today tend to score around 80% on average. Consider these scores and determine where human oversight is needed to validate AI-triggered responses. Also look for a solution that is continuously learning and calibrating to your environment.



## Compliance and data security

---

The best AI-based solutions ensure compliance with industry regulations by accurately monitoring and analyzing video data. This mitigates the risk of fines or penalties.

By focusing on these key areas, you can cut through the AI hype and choose a video surveillance solution that truly enhances your operations.

## Chapter 7: Conclusion

# Maximizing the value of your investment

Selecting the right video surveillance solution is a critical decision for enhancing security operations. By investing in a forward-thinking technology partner, you address current security challenges more effectively while positioning your business to take advantage of future advancements. Here are a few things to look for to ensure you are investing in the right partner:

**Openness** - Look for solutions that are open and easily integrate with other systems, ensuring flexibility and scalability as your needs evolve.

**AI-powered solutions** - look for a solution that extends the utility of surveillance beyond traditional security measures and is thinking long-term about the benefits AI can bring to a business to solve both security and operational challenges.

**Cloud native solutions** - Cloud native systems offer scalable and adaptable solutions that evolve with technological progress, safeguarding your data, and ensuring your investment remains relevant.

**Superior customer experience** - The value of a software as a service (SaaS) is the added benefit of customer support. Look for a vendor that truly cares, and is willing to work with you over time to ensure you continue to gain value from your investment. Also be aware of vendors that lock you into long contracts as this means they don't necessarily have to earn your business every day.

**Rapid pace of innovation** - Ensure your solution is future-proof by selecting a provider that offers frequent updates to keep your technology cutting edge.

While no single solution is universally suitable for all businesses. An ideal video surveillance solution embraces openness, flexibility, reliability, and ongoing innovation. By carefully evaluating these factors and aligning them with your specific business requirements, you can mitigate security risks and protect your assets, employees, and customers in an increasingly digital and interconnected world.



## ABOUT ARCULES

Arcules is aiming to set the standard for agility, security, and analytics for video surveillance in the cloud. Whether you resell, offer consulting and integration services, you will have access to a collection of resources to ensure your status as a trusted advisor to your customers and prospects.

## CONTACT US & SHARE

Do you have the right partner to help you on your journey to a modern physical security infrastructure? We'd love the opportunity to discuss your unique needs and guide you on your journey.

[Book a free consultation](#)

Like this study? Why not share.



Arcules  
17875 Von Karman Avenue, Suite 450  
Irvine, California 92614  
[info@arcules.com](mailto:info@arcules.com)  
[arcules.com](https://arcules.com)