

The Growing Need for Scalable Data Storage in **Video Surveillance**

Introducing a revolutionary all-in-one solution that scales as your data grows



00 Executive Summary

Video surveillance systems are used in many industries today. In addition to the goal of increasing security in the company, there are different motives for introducing video surveillance, such as access control or quality assurance. However, all companies face the same challenges when it comes to data protection, security and integration.

The importance of video surveillance for a growing number of companies requires a close examination of data management infrastructure. In view of increasing data volumes and stricter legal requirements, linking existing video systems with a secure data storage solution is becoming increasingly relevant.

Future developments must also be kept in mind, as data volumes will continue to increase, making scalable storage a business necessity. **Impossible Surveillance Cloud** powered by Tiger Technologies offers an integrated data management and cloud storage solution that is secure, scalable and cost-effective.

01 More than just security: video surveillance as a multi-layered concept

Video surveillance is often associated with security companies or control measures, but it may make sense for *any* company, organization, or institution – be it an authority, an office or a club – to use video surveillance for their own security.

The most common use case for video surveillance is security. Any company may use video surveillance to protect itself or its premises, often in combination a Video Management System (VMS). Video Management Systems are software platforms for managing video surveillance cameras and other security components.

Security is central to most video surveillance applications but there are other applications as well. Surveillance cameras protect against break-ins, theft and vandalism, but are also used for access control and have a wide range of additional applications, i.e. liability protection, workplace control and customer service improvement.

Video management systems also play a role in emergency management by providing real-time information about events such as fires or natural disasters to enable faster responses. There are numerous video management systems that support a wide range of real-world applications.



02 Data Protection Dilemma: The balancing act between surveillance and privacy

In the European Union as well as in other countries, compliance with data protection guidelines must be taken into account for any use of video surveillance.

According to the European General Data Protection Regulation (GDPR), video surveillance of employees or other people is not automatically permitted. Because video images of people can be used to identify individuals directly or indirectly (i.e. in combination with other information), it is considered personal data. Observation during work, for example, represents a significant infringement on the personal rights of employees. However, under certain conditions, video surveillance can be justified if there are important reasons for it. It is therefore crucial for businesses to establish video surveillance applications in accordance with data protection law.

In general, the following aspects of data protection should be taken into account:

When it comes to **data capture**, the appropriate use of cameras requires intelligence and targeted identification of security problems. This minimizes unnecessary recordings, which not only protects privacy, but also reduces unnecessary data via more targeted and efficient use of video surveillance.

Storage period also plays an important role. While installing cameras may be justified for security reasons, timely and automatic deletion of footage is essential. Every company, agency or body should establish clear policies regarding video surveillance on their premises, including retention periods.



The **right to information** must also be observed comprehensively. People affected by video surveillance must be informed about the surveillance, its purpose, and how long the video data will be stored when the systems are activated.

Compliance with data protection guidelines is mandatory for every company that uses video surveillance technology. The equally essential task is to find a solution that can accommodate technology advances and growing data volumes while minimizing data storage costs.

03 **Clear perspective: Focus on video surveillance technologies**

The above mentioned points - technology, data volume, and cost - spotlight the importance of reliable, affordable and secure data storage for companies that utilize video surveillance. Video surveillance is a complex topic that is constantly evolving. The same applies to data storage. Given their interdependence, both technologies should harmonize as perfectly as possible.

If a company already has a video management system but is looking for new data storage, system compatibility is of course a priority. This is especially true if the surveillance data was previously stored locally and will be migrated or backed up to the cloud.



As a general rule, companies should consider the following points when selecting a data storage provider.



Easy integration

Choose a solution that allows for easy integration without disrupting the VMS. The installation should be fast and smooth without affecting ongoing operations.



Instant access

Ensure any video surveillance stream is accessible from any location in seconds.



Ironclad security

Ensure the solution offers robust data protection, disaster recovery, and regulatory compliance in a multi-layered security architecture.



Transparent pricing

Not all cloud pricing models are optimized for video surveillance. Choose a provider that is open about data download fees (egress fees), data transfer fees, API requests, and long-term storage additional costs.



Budget-friendly scalability

Larger video files and longer retention periods result in an increase in data volume and higher storage costs. Choose a provider that offers budget-friendly scalability to address these challenges.



04 Data dialogue: Precision is required when exchanging information

If a video management system is already in use and the surveillance data is to be stored in the cloud, the data must be transferred securely. For this purpose, cloud bridge software plays a crucial role in establishing this secure connection.

Cloud bridge software enables the secure transfer of video recordings from local recording servers to the cloud, and may also play a supporting role in migration processes. In today's business world, many companies no longer work exclusively with a single cloud platform and instead use services from different providers. Cloud bridge software helps manage and orchestrate these complex multi-cloud environments.

It's important to emphasize that the functionality of cloud bridge software varies depending on the provider. When selecting a cloud bridge solution, companies should therefore take their specific data management and storage requirements into account in order to select the right solution.

An additional point to consider is the integration between the cloud bridge software and the data storage solution.









To illustrate the points above with an example, [Tiger Surveillance Bridge](#) is a leading cloud bridge software that connect local storage with any cloud storage. The solution is designed to be extremely easy to install and configure and doesn't cause any changes or disruptions to the existing system. It's easy to use and also works around unstable Internet connections. In addition, it is very resilient and safe.



05 Retention analysis: Security as an all-round concept

When it comes to storing data in the cloud, security is a key consideration in addition to the requirements already mentioned. It is highly advisable to take a close look at the security measures that a service provider offers when storing data. If the following requirements are met, your data is in good hands:

-  **Multi-level encryption:** By default, every file is encrypted in transit, at rest, as well as on the server and optionally on the client side.
-  **Identity Access Management (IAM):** IAM enables the creation of multiple users, access keys, sub-users and groups with individual access rules.
-  **Programmatic IAM:** This feature allows Identity Access Management to be controlled entirely via the command line (CLI).
-  **Versioning:** This feature makes it possible to track all file updates, save a copy of each version and revert to previous versions at any time.
-  **Multi-factor authentication (MFA):** Enabling MFA further secures access to important files and objects to prevent malicious actors from accessing the data.
-  **Cross-origin resource sharing (CORS):** This feature protects data from malicious access from the Internet, such as cross-site scripting (XSS).



Impossible Cloud provides robust ransomware protection. A decentralized network of world-class data centers and a continuous testing and repair process minimize network vulnerability to keep data secure and available at all times. This distributed network architecture eliminates single points of failure, effectively preventing ransomware attacks.



06 Scalable storage solution: Impossible Surveillance Cloud as the key to secure video data retention

The guidelines and criteria for selecting a video data management and storage provider lead us to the conclusion that a secure, scalable, and compliant end-to-end solution is needed to manage, migrate, and store surveillance data.

Impossible Surveillance Cloud powered by Tiger Technology is a such solution and represents the perfect data management and storage solution for any existing surveillance system.

This combined solution seamlessly integrates Tiger Surveillance Bridge with Impossible Cloud Storage. Your video surveillance data is transferred via Tiger Surveillance Bridge from your VMS to Impossible Cloud, where it is securely stored in GDPR-compliant data centers. Impossible Cloud's decentralized architecture protects your data from cyberattacks and outages, and surveillance video footage is immediately available whenever you need it.



Impossible Surveillance Cloud (ISC) is a bundled offering that combines Tiger Surveillance Bridge with an Impossible Cloud Hot Storage subscription for seamless surveillance video management and storage. Tiger Surveillance is the leading provider of data management and security software for video surveillance, connecting each VMS on a local recording server to an Impossible Cloud Storage Bucket. With Impossible Surveillance Cloud, you can scale your video surveillance solution without the need for an upgrade or disruption of operations.

 Tiger
Surveillance Impossible
Cloud

Impossible Surveillance Cloud offers the following benefits:

 **Security**

Impossible Surveillance Cloud provides robust security with comprehensive protection against ransomware and cyber attacks through strong protection measures and the reliability of redundant, world-class data centers.

 **Performance**

The lightning performance of the Impossible Cloud Storage solution is reflected in fast upload and download speeds as well as real-time processing. Industry-leading availability ensures continuous access to your surveillance video data.

 **Integration**

Seamless integration between your existing VMS and Impossible Surveillance Cloud provides quick setup, easy maintenance, and flexible user management.

 **Price**

Impossible Surveillance Cloud enables you to reduce cloud storage costs by up to 80%, representing a significant savings over time as data volumes grow. Pricing models are transparent with no hidden fees or added charges for API calls.

 **Scalability**

Impossible Cloud's transparent pricing models make it easy to scale as your data volume grows.

Is your business facing growing video data volumes and rising costs?

Discover Impossible Surveillance Cloud today! Our video surveillance experts are here to support you.

[Learn more](#)

