White paper

5 technologies for safer data centers

November 2018

AXIS COMMUNICATIONS

Table of contents

1. Introduction

From online retail and mobile banking, through to cloud business productivity applications and digital infrastructure management, there is now an abundance of data that needs to be managed and stored in data centers. However, the increasing value of information has made data centers a prime target for nefarious intentions, from criminals stealing data for profit, to individuals wishing to disrupt business operations. Therefore, it has become increasingly important for organizations to ensure data centers are protected to a high level.

One way to protect this critical information is implementing a highly efficient data center surveillance system and protocols, a field in which Axis Communications is a global leader.

The evolution of technology and the advent of IP access control, IP audio, software and video analytics, now mean there are more possibilities for better operational efficiency within data center video surveillance.

This whitepaper presents how the main challenges faced by data centers can be solved using smart technologies in network video, audio, access control and analytics.

2. Perimeter and internal protection

The location of a data center is carefully chosen to reduce risks – ranging from climatic adversities, such as tsunamis and earthquakes, to invasions. Some of them are located in isolated places, which are difficult to access, so the mere approach of a stranger may indicate a potential risk.

Nowadays, to be pre-warned of intruders in remote locations where there are not guards patrolling the site, it is feasible to receive a warning via a smartphone if someone approaches the walls of a data center. The operator in the control office is automatically warned and can access a visual of the suspects right away, day or night. If a threat is detected, such as someone trying to jump the walls, advanced technology can react with more powerful alerts, like a sound message using IP horn speakers.

Assault strategies are evolving, so a perimeter breach may also take place above the fence, using drones. Just as the internet opened up a new way for hackers to harm organizations, drones have enabled similar situations such as corporate espionage, terrorism and hacking. As a result, drones now represent a serious new security threat to data centers. These installations now face the risk of having its systems disrupted or suffer physical harm. One-way data centers are addressing these sorts of attacks is the use of air protection technology – combining cameras with specialist drone detection software to create an early warning system. The combined solution can detect drones and protect high-value airspace from drone threats, even when the aircraft is operated by GPS coordinates.

On the other hand, for the people who actually access the data center, it is recommended that they monitor who is entering, together with a time recording. Furthermore, it is useful to track how much time they remained there, and which areas were accessed. Many technologies address this type of control. Some data centers not only use systems based on a password or card, which always bear the risk of being copied, but also some type of physical verification, like facial recognition. This can be done by employing video intercoms (preferably resistant to acts of vandalism for external areas) with a facial recognition software. When the face matches with the one on record, and when the schedule corresponds to the authorized time frame, the door opens using network access controllers.

In fact, the access control system goes beyond the main areas. It can also include smaller rooms and even doors of racks. Certain intelligent modules can connect to I/O devices in order to generate alerts, for example when the door of the rack is left open. At the same time discreet cameras can help to keep unauthorized people from opening the door during unusual times.

3. Process analysis and protocols compliance.

Upon entering the data center, the challenges continue. After all, we are dealing with a physical environment that requires the compliance of protocols. Only in this way, is it possible to guarantee excellence in the management of its infrastructure. In these environments, it is usually forbidden, for instance, to use smartphones with cameras, and many data centers limit the number of persons who are allowed to enter at the same time.

An intelligent video surveillance system can detect the exact number of people who are currently in the monitored area and immediately send out an alert if the allowed quota is exceeded.

Besides the amount of people, this analytic, which is embedded in the camera, also reports the average period of occupancy. If a third-party professional, for example, usually takes 30 minutes to fulfil a task, the system can be programmed to send a notification should someone stay longer than that time frame. This feature can be useful for data centers, because they typically have periods, during which nobody is supposed to access the premises.

These and other occurrences, like an abandoned object on the floor of a corridor, can trigger warning sounds using IP loudspeakers. These messages are useful to dissuade malicious persons as well as to caution against the employees' carelessness. Indeed, a study by CompTIA[1] (Computation Technology Industry Association) showed that 42% of the surveyed safety faults could be traced back to either a lack of attention by the end user or failure to meet protocols.

[1]Trends In Information Security Study:
www.comptia.org/resources/trends-in-information-security-study

It's even possible to program recurrent warnings to serve as a reminder to the people in charge, so they can fulfill a task. These are all intelligent measures to reinforce the fulfillment of protocols and reduce risks in a critical environment.

4. Efficient data management from the video surveillance system

In recent years, data centers (especially those of major size) have invested in optimizing energy consumption. This has been achieved through the use intelligent strategies for refrigeration alongside efficient software for energy management and by using fewer servers to process the same amount of data. The same logic can be extended to video surveillance devices.

All the devices connected to a network generate information that must be handled. To do so, an efficient data center must consider two factors: the amount of information that it manages from cameras up to the servers, and the required storage for its preservation for a certain period.

Therefore, efficient data management is essential. The H.264 standard (which is the format most commonly used for the recording, compression, and distribution of video content) offers a significant image compression, which can be increased by technology like Axis Zipstream. It provides various methods for reducing the video bitrate without visible loss of quality. By doing so, up to half of the amount of bandwidth is needed – a significant reduction compared to systems limited to H.264.

Consequently, the information that is stored also halves. Using the H.264 standard, video recordings with 20 frames per second in high definition (1280 x 1024) last only 28 days with a storage of 2 TB[2]. By adding Zipstream, this storage can be extended to 56 days without losses – or one can invest in a cheaper, 1 TB storage to reach the same 28 days.

Apart from the compression, there are other ways to reduce data flow from video surveillance systems. One way is to adjust the image format so it fits the observed area. For instance, instead of generating an image in landscape mode, if looking at a corridor it would make more sense to change it to a vertical image.

A vertical view offers more details at the end of the corridor. This allows for a single camera to cover 50 meters. By reducing the number of cameras, the data center can also reduce the amount of stored video material to the half. Combined with compression technology, the data amount can be reduced by 75% on average.

[2] Video Surveillance Storage: How Much Is Enough?
www.seagate.com/files/staticfiles/docs/pdf/whitepaper/video-surv-storage-tp571-3-1202-us.pdf

Another well-known concept is edge storage. The camera installed at the door of a rack or in the ceiling of the data center can contain a memory card (e.g. 128 GB) optimized for video surveillance. Using motion detection as a trigger, the data center can easily spend 51 days before the information on the SD card is overwritten. The video stream is not transferred over the network. For data centers with higher safety requirements, the same concept can also be used for redundancy., meaning that video footage is stored in two places, on the edge as well as on central storage.

5. Health monitoring and cybersecurity

If data center walls and air space are protected, and if the access control is smartly working, and the amount of information and storage is minimal, it seems like everything is under control, right? Absolutely not.

In 2015, CompTIA flagged in a report, called "Trends in Information Security", that 85% of the successful data breaches targeted the top 10 known vulnerabilities. Despite the fact that the necessary software has been available, these weak spots had never been patched

To make matters worse, 83% of data breach victims took more than a week to detect a violation. The consequences of this can be calculated in dollars. It is considered that the 2013-2014 attack on almost 3 billion of Yahoo users' accounts have harmed the sales value of the company in 350 million dollars.

This is why it is essential to monitor the health of systems in a data center. Companies and government organizations that manage their own data centers can take a better control of their installations using device managing software, which constantly analyses the health of all devices connected to the network: cameras, access control, audio equipment, and so on. Firmware updates are automatic.

Some certifications request, for instance, that the devices connected to a network, not only come already set from factory, but also with the embedded certificates demanded by the client. To meet such a level of demand, it is possible to ask for customized firmware for a specific project.

6. Unified management

It's easy to see that these technologies point in the same direction. The most advanced data centers around the world already benefit from the new possibilities of integration among different devices that are connected to a network. It becomes increasingly evident that a centralized management of systems is extremely efficient.

Take, for instance, the entrance of vehicles in a data center: a vehicle approaches the camera detection area, placed at a car entrance. Then the embedded software verifies the license plate. The camera sends the number to an access controller, which checks if the vehicle is allowed to enter. For a higher level of security, a video intercom installed at the same height as the driver can request a QR code, which can be received via smartphone in advance. To finish the process, the door opens and the sequence of events is recorded and stored. Again, safety and access control take joint action.

In a totally IP environment, where even audio devices use the SIP protocol to communicate with IP phones, a data center can quickly share information and operate with efficiency.

These benefits tend to be greater for those investing in open hardware and software technologies, for they can be easily combined with other technologies. This is why organizations such as ONVIF, which work in favor of interoperability, continue to fuel innovative solutions. They are especially needed to solve different challenges in data centers, where the physical, virtual and access control safety are interconnected by nature.

72743/EN/R1/1811

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems. Axis has more than 3,000 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website www.axis.com.

AXIS COMMUNICATIONS