Data centers

Axis magazine, Issue 1

How Axis is improving security and operations

Enhancing and improving data center security using a five-layered approach

Security in 3D: How rising drone use is ushering in a new threat vector

Helping data centers improve their green credentials

and more!

AXIS COMMUNICATIONS

Editor
Sienna Dzanic
Global Enterprise Marketing Manager
sienna.dzanic@axis.com

Contents

More people than ever before are reliant on the data center as modern behavior patterns stimulate our growing appetite for data. Advancements in artificial intelligence (AI), the advent of 5G, video-on-demand, and an ever-increasing number of IoT devices only add to the challenge.

Yet, as data centers grow and are more widely distributed, monitoring their operations and keeping them secure can prove increasingly difficult. At Axis, we've been using our expertise to work with data center leaders across Europe and helping them in many different ways. In this magazine, we will explain some of the issues to be addressed and the role that technology can play to provide support.

Improving site security using Axis five-layered approach
The Axis five-layered approach to security covers perimeter, premises, buildings, server rooms, and server racks. Using network-enabled video surveillance with edge-based analytics, Axis is able to deploy a truly intelligent physical security solution to improve security and transform operations for greater resilience and efficiency.

Detecting drone activity to mitigate risk
The presence of drones within the vicinity of the data center is a growing risk that should be prompting data center managers to stop thinking about security solely in two dimensions and ensure tighter air-space defense. The use of dedicated software to detect drones based on the radio frequency (RF) signals that they emit is complemented by Axis network camera technology, providing operatives with advanced warning of a drone approaching and indications of its intent.

Reducing carbon footprint and achieving green targets
Data center operatives need to be looking forensically at the systems, products, and materials used in order to make small, but incremental gains towards reducing carbon footprint and achieving sustainable targets. Trusted partnerships, the use of renewable materials, and the right technology can lead to greener and more sustainable data center operations, which Axis is well positioned to support.

Digital transformation and the role of the network camera
Data centers can combine existing sensor technology to improve operations based on advanced business intelligence. Data generated by Axis cameras, used as intelligent sensors, can be integrated into modern data center infrastructure management (DCIM) systems, leading to efficiencies such as improving cooling solutions. Well-informed engineers are able to act immediately to rectify any issues when armed with accurate information.

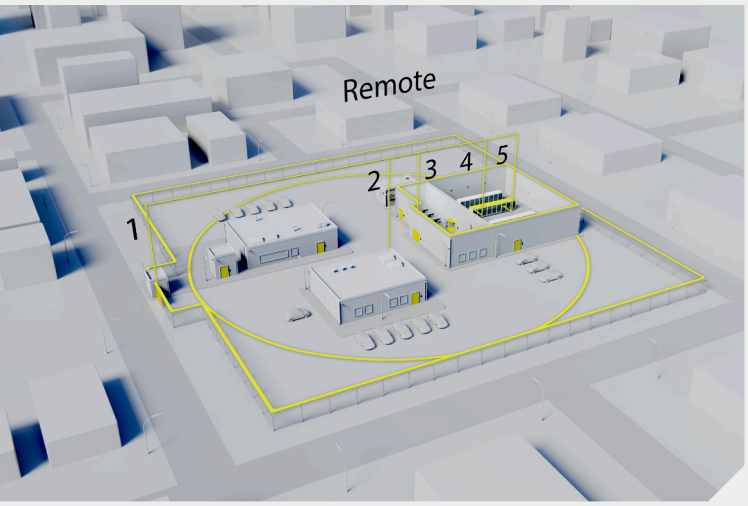
How to improve physical security through device interoperability
An increase in physical threat is prompting the use of innovative, connected technologies for a smarter approach to data-center security. Axis physical security solutions can play a vital role in securing the data center through their ability to effectively talk to each other, resulting in a truly intelligent, largely autonomous system for maximizing data center defence.

We hope that the substance of our magazine is useful and will provide food for thought. Whatever the challenge, Axis is committed to working with its partners and customers to develop cutting-edge solutions for the creation of a smarter safer world.

Wishing you a successful year ahead,
Peter Dempsey, Key Account Manager, End Customers – EMEA

Enhancing and improving data center security using a five-layered approach

The growth of cloud services and hyperscale computing means that more people than ever before are relying on the sheer power and capacity that data centers provide. And consumption of data is growing rapidly as a result of modern behavior patterns.



As data centers grow and are increasingly spread out, monitoring operations and guaranteeing high levels of security can prove challenging, with personnel under increasing pressure to guard against threats both physical and cyber in nature. Any disruption to operations could prove catastrophic, with periods of downtime having significant cost implications and causing massive disruption to the people and businesses that now rely so heavily on this seamless transfer of data as part of day-to-day living. It is therefore essential that appropriate tools and technologies are put in place to provide comprehensive, overarching protection, and that such solutions are fully scalable as data centers continue to expand and evolve.

Comprehensive site security – inside and out

Axis integrated video and audio solutions can be employed to protect data centers and ensure smoother operation. Our five-layered approach covers perimeter, premises, buildings, server rooms, and server racks, using network-enabled security products with edge-based analytics, resulting in a truly intelligent solution that offers comprehensive end-to-end protection. Detecting and resolving incidents becomes straightforward, and the potential to apply a range of cameras and sensors will give operatives complete peace of mind. the trigger for a smart city adoption and the direct route to a more liveable city.

Axis network video and audio helps protect the perimeter of the data center by utilising video surveillance cameras, thermal cameras and radar to detect movement at or near the site, tracking intruders that are approaching on foot or in a vehicle. Automated alerts and alarms can be triggered through network speakers to deter potential criminals, and these can also be used by operatives to address intruders directly in real time. Such technology, driven by powerful analytics, has high levels of accuracy, resulting in fewer false positives and subsequently representing cost savings.

At the premises, access control systems using video surveillance as a second factor of authentication are employed at all entrance points to identify, authenticate and authorise, with facial recognition analytics also used to manage entry to buildings, rooms, and even individual server racks. Network audio can also play a role in protecting against crime from internal sources, with alarms and alerts triggered by network cameras monitoring for unusual activity within the data center's many buildings. Such activity might include a server rack being accessed without authorization or attempts to access controlled areas at unexpected times.

With so much data at stake, having a system that is highly secure but also fully scalable as the data center grows is absolutely imperative. Any device that is left vulnerable could be compromised, either by inside threat-actors or those attempting to gain access from outside. Axis addresses these issues by continually hardening cybersecurity on devices with firmware upgrades, updates and maintenance tests.

Axis is ideally positioned to help the modern data center secure its assets and protect its premises, with a host of network solutions that offer encrypted communication, IP address filtering, secure boot, and signed firmware. The Axis approach ensures that cybersecurity is not an afterthought, but something that is factored in right from the start.

5 layers

- Perimeter
- Premises
- Buildings
- Server rooms
- Server racks

Supporting data centers on the digital transformation journey with network cameras

Data might be the most valuable strategic resource we have, but only when it's used effectively. Although siloed data helps keep individual systems simple, it also represents a missed opportunity. Unity of data is the key to creating truly powerful business intelligence.

This integration of data and the linking together of sensors and actuators with AI generates actionable insights that can lead to significant operational efficiencies across a wide range of industries and sectors.

Properly analyzed data connects services with the people that use them, integrating a broad system into an efficient whole. So, why isn't this always the case in the data center? Today's climate is one of increased scrutiny over energy efficiency, asset security, and service quality, in which data centers must also deal with increased processing and heat requirements as customers demand ever-more-complex data analysis. Building security and hardware management often exist in separate silos, yet data centers need to make use of every possible resource available to them if they are to meet demands.

The new smart networking paradigm

Thankfully, the need for alignment comes at a time when the tools to make it happen are more readily available than ever before. Internet of Things (IoT) devices now have more power to collect, process and analyze data internally. Working on the edge vastly reduces their bandwidth requirements, lowers external processing demands and reduces end-to-end latency from 100-250ms to 10-20ms* by simply taking out the need to continually send vast amounts of data back and forth to cloud servers.

IoT devices are, at last, speaking the same language as each other. The growing popularity of the Message Queue Telemetry Transport (MQTT) protocol, which sits on top of industry-standard TCP/IP networking, means integrating data from these devices into server or cloud-based applications is easier than ever before. MQTT is open source and based on open standards, which makes developing new endpoint integrations or automations based on its data straightforward. There is now no reason for a data center's security systems to exist on a separate network to its data center infrastructure management (DCIM) sensors.

The evolving role of the network camera

The open nature of MQTT offers the opportunity to integrate data which meets the demands of modern DCIM systems by using network cameras as intelligent sensors. Take, for example, heat monitoring. An internal heat sensor might notice a hot spot on a server rack and feed its data through to a thermal camera; that camera could then relay an image containing all relevant data to a video management system, giving an engineer a true visual indicator of where the issue lies. A combination of data from a variety of sensors may in turn lead to greater efficiencies, such as fine-tuning cooling solutions for optimal energy use.

Finding new ways of utilizing the data that network cameras collect is also an opportunity to vastly lower the cost and complexity of DCIM. Data centers are pushing to find efficiencies wherever possible, so the use of network cameras for a wide range of applications could be a shrewd move. In addition, those that already use cameras for security purposes can exploit the full potential of these devices for operational benefits, too.

The time has come for the truly smart data center to become the norm. This doesn't mean throwing out existing DCIM solutions or switching critical sensors – it simply means harnessing every piece of existing data to create new opportunities while making the most from cutting-edge connected devices and solutions.

*www.ibm.com/blogs/internet-of-things/iot-5g-transforms/

Security in 3D

How rising drone use is ushering in a new threat vector.

Drones are becoming big business as their legitimate function within enterprise environments delivers significant operational benefits. But their expected growth[1] will not be without its security drawbacks. During Christmas 2018, the UK's Gatwick Airport was closed for 33 hours affecting more than 140,000 passengers. Despite multiple eyewitness accounts, the presence of a drone could not be verified[2].

This highlighted a major problem. Perimeter protection methods were effectively bypassed by a drone, available for as little as £200, yet costing the aviation industry millions. And when one thinks of the possible payloads that drones are capable of carrying, ranging from a camera to conduct hostile reconnaissance, to equipment designed for hijacking a wi-fi signal to disrupt software and systems, or even a biological weapon, the issue is brought into very sharp focus.

Detect, identify and locate

Within data centers, guaranteeing high levels of security by guarding against threats both cyber and physical in nature, is a critical capability. Any periods of downtime would have significant cost implications and cause massive disruption to the people and businesses that rely so heavily on a seamless transfer of data.

Modern network-enabled systems bring considerable advances to perimeter protection capabilities incorporating video surveillance cameras, thermal cameras and radar to track intruders' movements. And while the data center has become infinitely more secure in recent years, being wise to new threats is the key to being one step ahead. The new threat may now come from the skies above.

The use of dedicated software to complement network-enabled physical security solutions now allows drones to be detected based on the radio frequency (RF) signals that they emit. This can be used to identify the make and model of more than 200 drones, including commercial, hobbyist and DIY, even pinpointing the location of the operative. Far more powerful than relying on the eyes and ears of security personnel alone, this technology can provide advanced warning of a drone approaching and early indications of its intent.

Drone use promises much when in the right hands, but as with many things, we should be wise to its pitfalls.

Drone analysis and threat mitigation

Once detected, it's important to establish the reason for a drone's presence. Data centers typically operate a no-fly zone, so security officers or police need to be able to very swiftly establish the difference between a careless drone pilot and a threat actor involved in malicious endeavor. By pinpointing a drone and detecting the signals given out by its operator's equipment, security personnel can be dispatched to have a conversation with the pilot.

Where an incident is verified, swift identification is imperative to aid early decision making. Drone detection software, capable of sending a signal to a PTZ (pan/tilt/zoom) camera can be used to lock-on to and track the movements of a drone, with crystal-clear imagery used to ascertain the substance of its payload to distinguish friend from foe.

A drone detection solution produced in partnership

With the threat presented by drone activity increasing, Axis and its partner Dedrone collaborated to deliver a unique industry solution for smarter airspace security. Data gathering is key to the solution's success, with over 17 million drone images so far being used to train camera-based AI/ML software to accurately identify drones, even when heavily disguised. Moreover, remote identification protocols, known as RemoteID, provide information to verify a drone's legitimacy. This also serves to enhance threat detection capabilities.

Drone use promises much when in the right hands, but as with many things, we should be wise to its pitfalls.

With such a solution in place, the skies around the data center can be monitored as successfully as the ground. Integration with existing video management systems also means that a drone detection solution can be part of an overarching and integrated system to improve security posture.

[1] www.insiderintelligence.com/insights/drone-industry-analysis-market-trends-growth-forecasts/
[2] www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone

Helping data centers

improve physical security

through device interoperability

Much has been written about the high levels of cybersecurity needed to protect data centers, and yet, physical security remains a concern. A story which made mainstream media in the US concerned the arrest of a man who allegedly masterminded a plot to blow up a major data center in Virginia*. When considering the action that should be taken to mitigate such threat, the introduction of cutting-edge physical security solutions is obvious. But what is not always apparent is the power that such solutions possess to secure and protect when interconnected to maximize defense.

Innovations in radar and network video

Network cameras have already evolved to the point where onboard analytics can be used to categorize motion (i.e., intrusion as opposed to loitering) and to differentiate people from vehicles and objects at the perimeter of a site. Such is the accuracy of modern cameras that numbers of false positives are greatly reduced. Additionally, edge-based processing ensures that only the most necessary data is passed back across the network for analysis, aiding swifter decision making and saving of time and money.

While physical security solutions can play a vital role in securing the data center, it is their ability to effectively talk to each other that results in a truly intelligent, largely autonomous system. As an example, a combined radar and camera solution can detect and classify movement at the edge of the perimeter, which in turn triggers a thermal camera to detect a heat trace and further evidence of unauthorized human presence. Next, a pan-tilt-zoom (PTZ) camera is employed for movement tracking, while an IP audio speaker plays a pre-recorded message to deter. An IP strobe siren is activated as the intruder continues to advance, delivering a simultaneous pulse of light and burst of sound as a final warning.

Of course, threat can come from other factors. Inside the facility, network cameras running an analytic at the edge can be used as the first port of call to detect gas leaks or smoke, while connected cameras and sensors can identify water leaks.

*www.bbc.co.uk/news/technology-56719618

Thermal metric cameras can play a critical role in detecting any rise in ambient temperature which might indicate a larger problem. When used to monitor power generators, for example, the slightest temperature fluctuation will result in an alarm sounding once a predetermined temperature threshold is reached.

Partnerships for comprehensive protection

The Centre for the Protection of National Infrastructure (CPNI) has developed guidance and standards for all critical national infrastructure sites; this would include data centers due to their delivery of services which are deemed essential. Partnering with a trusted vendor of physical security solutions that have been CPNI approved will provide data center managers with assurances that the products they choose are of the best quality and deemed capable of meeting high standards.

By selecting tools that are also at the cutting-edge in terms of innovation, data center sites will benefit from connected autonomous physical security solutions that provide protection at the very highest levels.

Helping data centers improve their green credentials and become more sustainable

The global green data center market is expected to reach $142.8 billion by 2026 at a near 20% CAGR[1]. For those data centers, getting it right means being able to offer robust and highly secure storage while optimising energy efficiency to ensure low environmental impact. This is particularly critical in light of the Climate Neutral Data Center Pact's commitment to make data centers climate neutral by 2030[2].

Yet for many data centers, becoming sufficiently sustainable demands a considerable rethink. Concerns turn to the vast amount of energy used and heat generated, and how to address the impact on the environment. Understandably, there is a mounting pressure on data centers that are not already operating in accordance with sustainable initiatives to become more focused on meeting green targets. For the data center manager, the challenge is to improve sustainability while continuing to offer the best service.

Sustainable frameworks and trusted supply chains

Demonstrating a greater awareness of the impact that positive actions can have for the environment will attract businesses with a similar commitment to sustainability[3]. Working to international frameworks and standards such as the UN Global Compact, of which Axis is a signatory[4], can play a role in helping companies achieve the UN's sustainability development goals (SDGs)[5] as well as offering proof that a business is demonstrating commitment beyond mere words.

Indeed, adherence to internationally recognized frameworks also speaks of shared values. With a closer focus than ever on driving cost efficiencies, accessing high-tech skills, improving service delivery, and driving innovation, the need for partnership working is key. As organizations seek closer working alliances, all stakeholders in the supply chain should be aligned around core values to build trust.

Reducing carbon footprint and achieving green targets

Data centers use a considerable amount of power and generate high levels of heat, causing concern among green-focused data center managers. While there is no simple, quick solution, data center operatives need to be looking forensically at the systems, products, and materials used in order to make small, but incremental gains towards reducing carbon footprint and achieving sustainable targets. This might include sourcing vendors for whom manufacturing with low-power consumption in mind is a priority.

For example, the use of edge-based analytics within Axis network cameras, which facilitates the processing of video data within the device itself, means that on-camera decisions result in a reduction in the bandwidth and power consumption that would be associated with the constant transfer of data back and forth across a network for processing. Axis Zipstream[6] technology improves bandwidth and storage requirements by an average of 50%, further supporting a greener business agenda.

Axis helps data centers improve their sustainability posture by offering innovative solutions that deliver the highest security with the lowest environmental impact. Careful selection of materials and a commitment to reduce waste in our processes demonstrates that we are serious about our responsibility through the whole chain of production. This is our commitment to support data centers in meeting their green targets while innovating for a smarter, safer and more sustainable world.

[1] www.kbvresearch.com/green-data-center-market/
[2] www.climateneutraldatacentre.net/
[3] https://on24static.akamaized.net/event/26/52/12/7/rt/1/documents/resourceList1601294964064/99821008210sustainabilityreport451researchen211601294962692.pdf
[4] www.unglobalcompact.org/what-is-gc/participants/1056-Axis-Communications-AB
[5] www.axis.com/about-axis/sustainability
[6] www.axis.com/solutions/zipstream

Recommended solutions for data centers

Axis
radar-fusion
cameras

Get wide-area intrusion protection and reliable 24/7 detection with a fusion of two powerful technologies: video and radar. This unique device provides state-of-the-art deep learning-powered object classification for next-level detection and visualization.

Axis
PTZ cameras

PTZ cameras deliver real-time monitoring for wide areas thanks to pan, tilt, and zoom functionality. AXIS Q61 Series provides full scene fidelity and perfect image quality in all directions – above as well as below the horizon. This makes the series uniquely suitable when there is slightly uneven terrain. AXIS Q62 Series includes heavy-duty cameras that stand up to all weather conditions. AXIS Q63 Series provides quick zoom and laser focus, even in the dark. With speed dry functionality, you get clear, crisp images even in rainy weather.

Axis
security radars

Axis security radar is a network-based device suited for area monitoring in low-speed areas (up to 55km/h~34 mph), or road monitoring in vehicle lanes with higher speeds (up to 105 km/h~65 mph). Using advanced radar technology featuring built-in analytics developed using machine learning and deep learning, it can accurately detect, classify and track objects of interest 24/7.

Axis
access control

Axis provides the hardware and analytics to identify, authenticate, and authorize entry to buildings and rooms. Our access control technology protects critical or vulnerable areas with automatic (key cards, PIN codes, QR codes) or manual authentication (2-way network video and audio).

Axis
network horn
speakers

Axis network horn speakers allow you to discourage unwelcome activity and warn off bad actors detected by your cameras. For example, the speakers can be used to deter unwanted presence/activity by a site's perimeter. The speakers can also be used to provide voice instructions during an emergency or inform about illegal parking.

Why Axis?

Driving cybersecurity

Cyberattacks on infrastructure or data theft can have catastrophic effects on a city. How vulnerable would we become if the cameras that govern traffic light signals were hacked? Mitigation of such threats is at the top of the agenda for authorities moving forward. Axis is a leader in security solutions with a superb track record in keeping smart city data safe, secure, and compliant. We have become experts at assessing risk and building processes for data protection into every level of our offering, always compliant with current and future policies, regulations, and legislation.

Quality in everything we do

At Axis, we always act and work with quality in mind. All our products are built to stand challenging conditions, being resistant to vandalism and harsh weather. Products have been extensively tested to last long and deliver sharp images in all conditions. Our quality thinking is evident in the excellent HDTV images that our cameras deliver – quality so high it holds up as evidence in court.

The power of partnerships

Axis open platform is flexible, scalable, and easy to integrate, being compatible with many different partners, third-party hardware, and software solutions.

Innovative technology

We constantly strive to combine the best of technology and human imagination to make our products perform better. The case for analyzing and utilizing data on the edge is rapidly catching on, and can give you actionable insights.

Learn more about Axis solutions for data centers:
www.axis.com/data-centers

About Axis Communications

Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.