

Data center magazine issue

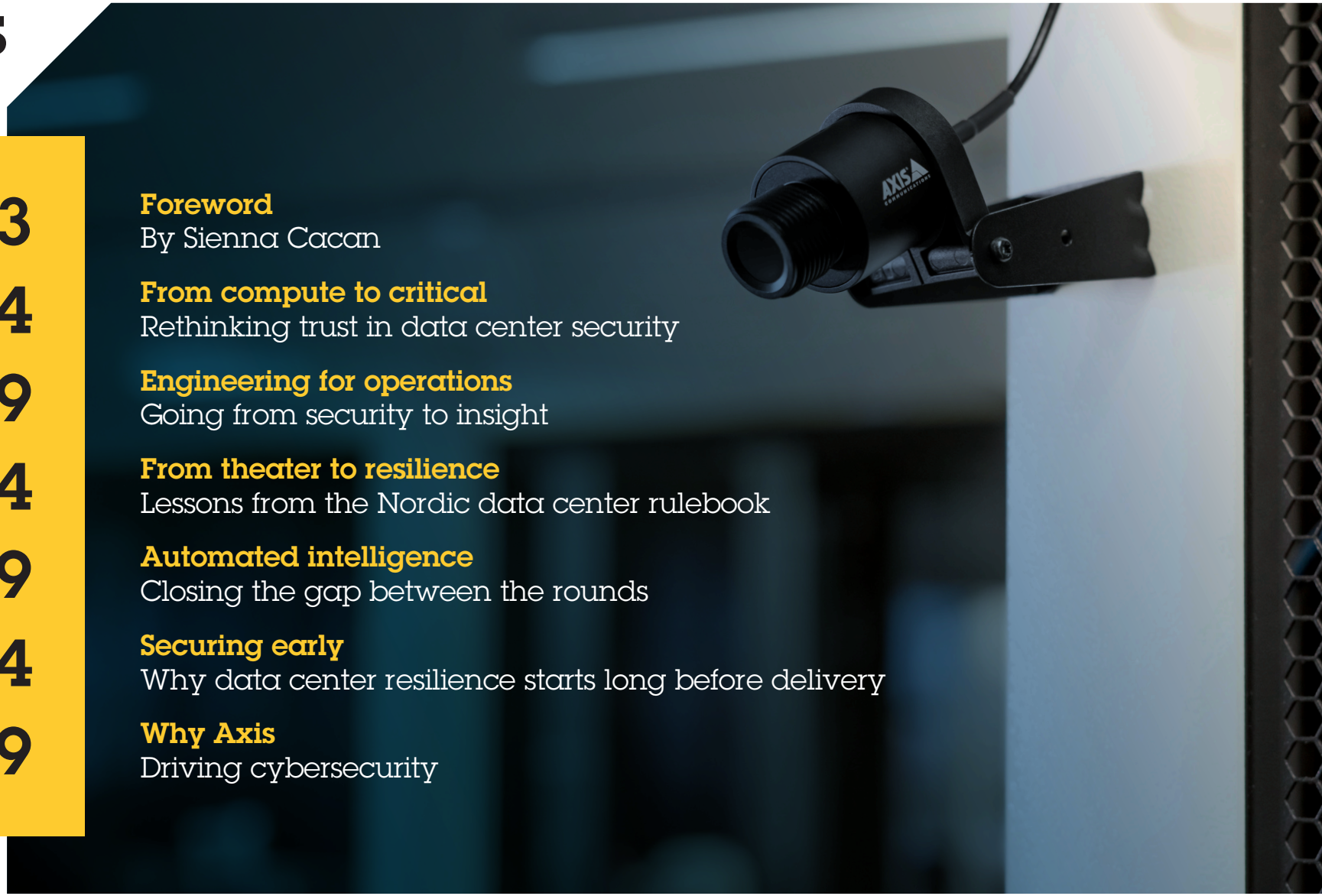
03

Engineering trust in the digital world

A data center can look secure and still be vulnerable. It can be built for scale yet struggle with resilience. As digital infrastructure becomes more critical, it is time to rethink the relationship between security, intelligence and operational performance. Explore five perspectives on closing the gaps, challenging convention and building resilience into every layer of the data center.

AXIS COMMUNICATIONS

Contents



03 **Foreword**
By Sienna Cacan

04 **From compute to critical**
Rethinking trust in data center security

09 **Engineering for operations**
Going from security to insight

14 **From theater to resilience**
Lessons from the Nordic data center rulebook

19 **Automated intelligence**
Closing the gap between the rounds

24 **Securing early**
Why data center resilience starts long before delivery

29 **Why Axis**
Driving cybersecurity

Foreword



By Sienna Cacan,
Global Enterprise Segment Marketing Manager
Axis Communications

The resilience shift: Rethinking how we secure and operate data centers

We are building a world that depends on data centers more than ever before. AI is accelerating demand, digital infrastructure is expanding at an unprecedented pace, and the systems underpinning our everyday lives are becoming increasingly interconnected. But as data centers grow in scale and importance, one question deserves more attention: are we rethinking how we protect and operate them at the same pace as we build them?

Resilience is no longer simply about keeping threats out or ensuring systems stay online. It is about seeing the bigger picture, understanding how risks connect, and making smarter decisions before disruption occurs. And that requires us to challenge some long-standing assumptions about the role of security in the data center environment.

In this edition, we explore what that shift means in practice. From rethinking trust and cybersecurity in physical security systems to embedding security into data center design from the outset, our contributors challenge conventional thinking. We examine the Nordic approach to integrating security with operational resilience, explore how connected intelligence can close visibility gaps between inspections, and consider why protecting critical equipment must begin long before a facility becomes operational.

Together, these perspectives point toward a common opportunity: to move beyond security as a protective layer and embrace it as an integral part of performance, resilience and operational insight.

The future of data centers will depend not only on how much they can process, but on how effectively they anticipate risk, connect information and maintain continuity in an increasingly unpredictable world.

We invite you to explore these perspectives and consider what they mean for the next generation of data center infrastructure.

From compute to critical: rethinking trust in data center security





Steven Kenny, Manager Architecture & Engineering Program - EMEA, Axis Communications, argues that in the age of cyber warfare, data centers need to build security visibility beyond their core systems.



Data center security has historically been seen in a technical, functional light. Select the right systems, meet the specification, pass the audit, and the work was considered complete. But data centers are more than they once were. As the world has become more connected, and as the importance of those connections has grown, so data centers have become critical infrastructure in the truest sense. They are foundational to economies, supply chains, communications and daily life.

Any failure or disruption has an immediate and meaningful impact both inside the data center and out. Accidents happen, but the cause of data center failures increasingly trends toward the deliberate. In today's geopolitical environment, critical infrastructure is an active target. Data centers are strategic assets. If they cannot be taken offline directly, they can be disrupted, observed, or undermined through cyber means.

Frameworks like the Critical Entities Resilience (CER) directive reflect a change in the way we think about risk, and a new emphasis on continuity, transparency and the ability to withstand and recover from deliberate disruption. Data center operators are, of course, aware of the value and vulnerability of their core systems, but it is arguable that the definition of 'core' needs to stretch far further.

The visibility problem

Surveillance and monitoring within the data center typically provides visibility and supports the appropriate response. Recent news, however, suggests that criminals have become far less likely to careen into a network with a loud attack. They increasingly use hostile reconnaissance techniques. These are used to quietly observe, map, and understand their targets from afar, or to establish a foothold for living-off-the-land attacks. Reconnaissance often extends over extended periods and is increasingly aligned with the objectives of state-backed actors.



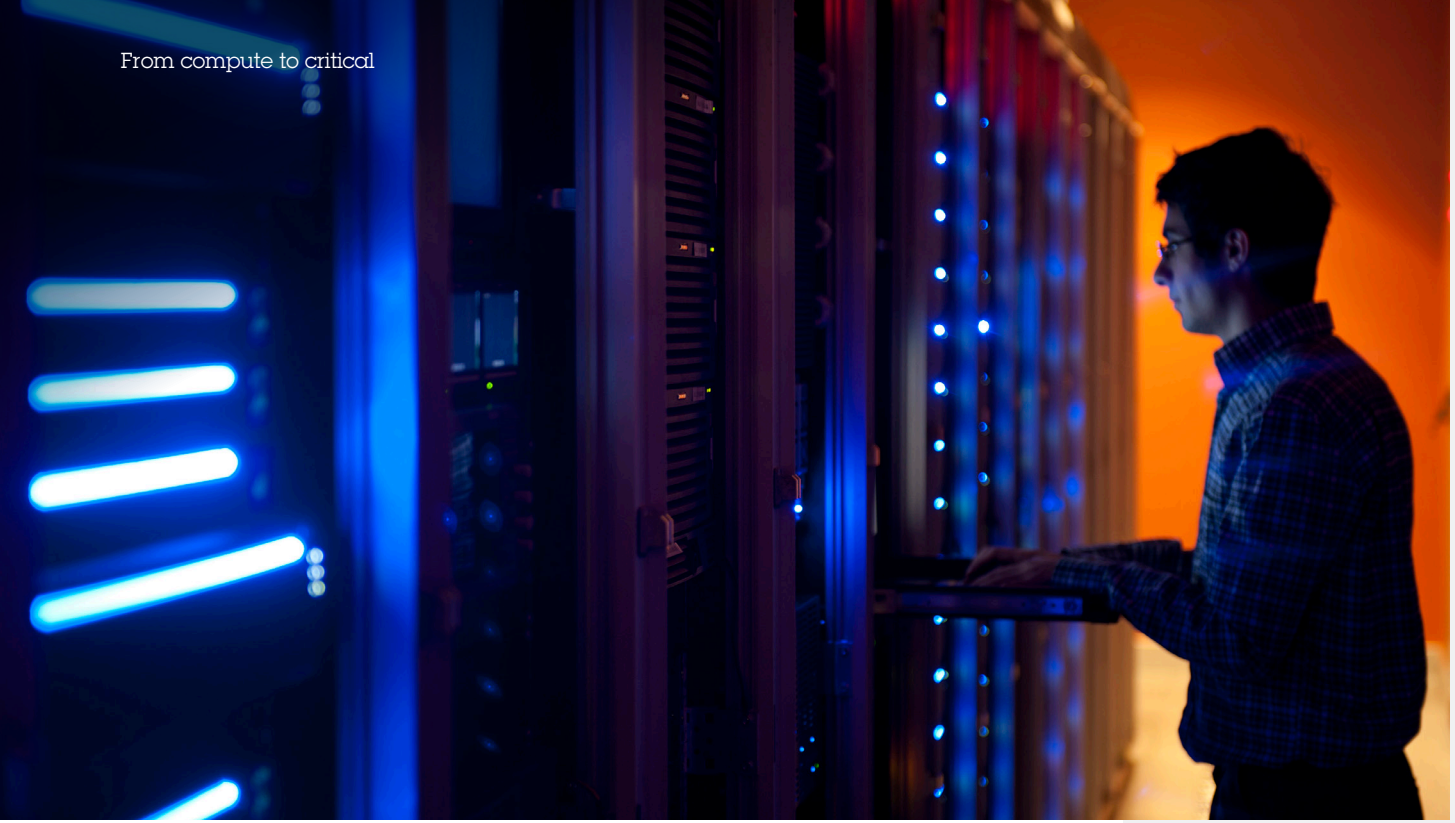
This places security and surveillance systems in a precarious position. Network cameras serve a critical function as the lynchpin of physical security and safety. But ill-secured camera hardware could also provide a hook for hostile reconnaissance, exposing infrastructure as much as it protects it. If data center operators focus on ticking boxes and hand-wave away the importance of selecting camera hardware which is robust, maintained, and integrated, they leave themselves open.

Security systems increase visibility for everyone, operational staff as well as those working in an adversarial capacity. Improperly protected cameras could provide attackers with an inconspicuous view of the physical layout and activities of the data center; poor cybersecurity could transform a single vulnerable device into a launchpad for a network probe or a direct route into even more critical systems.

The supply chain attack surface

Modern security systems are not static devices. They are networked, powerful, software-driven computers that never switch off. To treat them as a one-and-done, install-and-forget solution ignores the incredible potential they offer for both business intelligence and adversarial activity.

Data center operators know full well the level of caution that should be afforded to hardware that sits in the rack, and the same level of cybersecurity concern should be given to hardware outside of it. Due diligence has to be undertaken both on the security credentials of security hardware, and on the firmware and software which powers it.



> **"The conversation has to shift away from compliance and toward assurance. With data centers now critical infrastructure, risk has to be explicitly and continuously owned."**

Cybersecurity hygiene and geopolitics are more linked than it may seem. Technology is no longer neutral, because the supply chain is a significant source of risk. The delivery of what appears to be robust hardware on paper may not be what it seems if it has been compromised at some point along its chain of manufacture: a secret backdoor, a switched-out security chip, a rogue firmware update could be all it takes for a defensive tool to become an offensive weapon. In that context, the audit trail of a camera, or any product, is arguably as important as its final credentials.

Accountability first

Every device which enters a data center carries some level of risk, but responsibility for that risk is rarely clear. Engineers design systems to meet technical requirements, integrators deliver what is asked of them, operators keep everything running. Risks may be acknowledged at any of those stages, but rarely are they owned. Sometimes a conscious decision is made to proceed even in the face of known risks, on the basis of cost or timelines, or on the assumption that dealing with those risks falls outside the scope of the project.

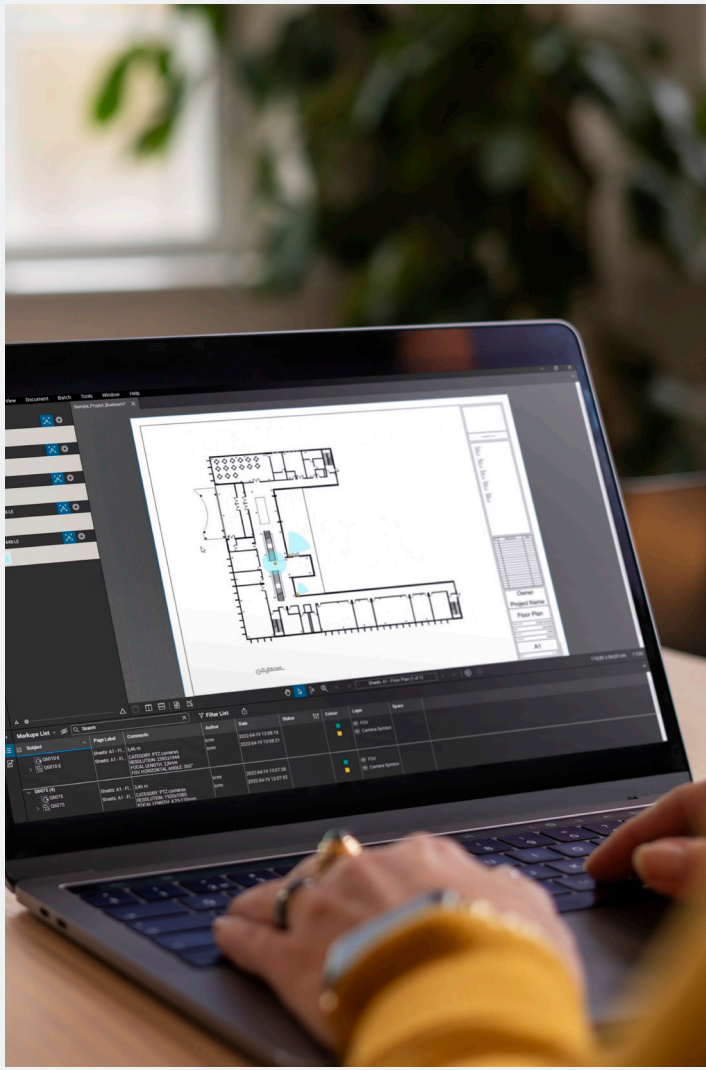
In many cases, the risk is not unknown. It has been identified, documented, discussed and, ultimately, accepted. This does not indicate negligence, necessarily, more a focus on performance and delivery over context. This is the critical gap that needs to be closed. With data centers now critical infrastructure, risk has to be explicitly and continuously owned. The conversation has to shift away from compliance and toward assurance.

Threat reconfigured

It is up to data center operators to understand how their systems work. That means working with architects and engineers who can offer them that assurance. Systems must demonstrably meet the required standard at the point of installation, offer the provenance and support that keeps them at that standard, and be able to remain under the technical and operational control of the organization in which they are installed.

Reaching that level is not a given, but it is made much easier when security systems are considered as equal to the headline infrastructure of data centers. That attention helps prevent the small assumptions, overlooked devices, and unchallenged decisions which create opportunities for attackers.

Ultimately, this is what resilience frameworks such as CER are attempting to address. Disruption does not have to come from a physical attack, so security considerations must extend beyond the physical. Security is a position, one that has to be taken deliberately and held, or data centers risk becoming the Achilles' heel of the world economy.



Back to contents ↑

Engineering for operations: going from security to insight



Tertius Wolfaardt, Architecture & Engineering Manager - South Asia Pacific, Axis Communications, discusses why security systems must be embedded at the earliest stages of data center design to support uptime, efficiency and trust.



Too often, security arrives late to a project. The core systems have been defined, the layouts fixed, the budget secured and allocated, and only then is the question of security systems addressed. And by that point, any answer is constrained by what exists and what the design allows. That is not a viable approach. Security systems influence the way complex environments like data centers and critical infrastructure facilities operate, how they are maintained and made compliant.

Security systems are a vital pillar which supports decision-making and safety, thus architects and engineers must consider security structurally, and do so early. **Security systems create a vital data layer. They should be treated as a core part of infrastructure considered alongside power, cooling and connectivity at the earliest design stage.** Introduce them too late, and they remain peripheral and unable to reach their full potential.

The power of procurement

In large part, security systems' current importance stems from their versatility. Physical security is, and will always be, a core function, but when cameras, sensors and analytics platforms are employed as data generators they create value. Businesses are more willing, and indeed likely, to invest in solutions that support business uptime, reduce total cost of ownership, or improve performance.

This shift in thinking toward business insight and operational efficiency changes the game. It puts consultants and manufacturers in the position of justifying what a system can deliver rather than just what it does, which in turn moves the position of influence in the product lifecycle. Security is a design decision, and it comes in early.



Consultants define requirements, shape specifications, and establish approved vendor lists. Integrators tend to follow those specifications. By the time a tender is issued, a system's delivery capabilities are largely set. Early-stage procurement is also the time to establish that a security system meets regulatory requirements, privacy obligations, and cybersecurity expectations, none of which can be retrofitted. In practice, this means defining risk levels, system requirements and integration points before design is fixed, ensuring that security is engineered into the environment.

System integration - by default

Early engagement also determines the way security systems are treated, whether they become isolated components or part of a broader operational structure. In data centers in particular, uptime, resilience and efficiency are constantly monitored.

The data from embedded security systems can be part of and contribute to building and energy management systems (BEMS), data center infrastructure management (DCIM) platforms, and wider operational workflows. Added later, those connections tend to be partial or missing altogether.

Looking through the lens of business insight highlights the possibilities. A camera purely positioned for perimeter monitoring serves its defined purpose; the same device, specified and located with intent, delivers more. It contributes understanding of the way a facility operates, generating data around patterns of movement, vehicle flow, access frequency and dwell times. It provides a reference point for informed operational decision-making.

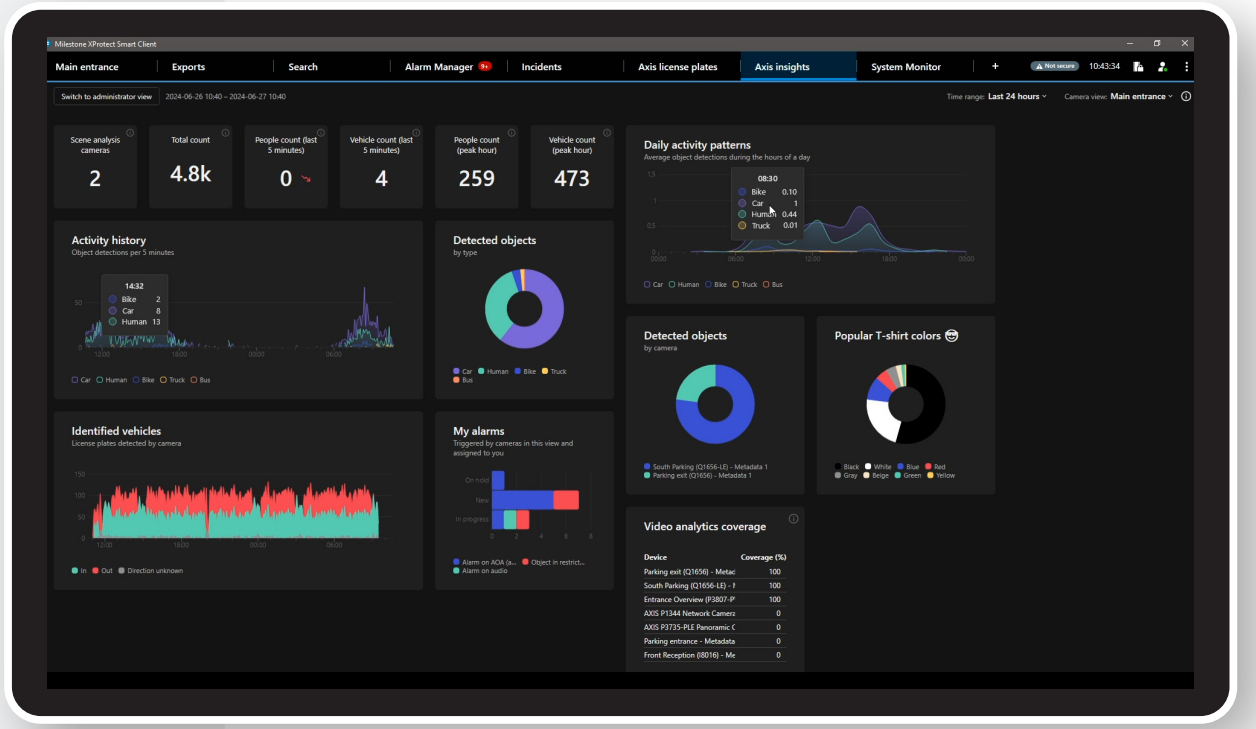
Intelligent system building

The way architects and engineers think about risk is changing. Traditionally, risk in physical security has been event-driven and almost retroactive, centered around unauthorized access, intrusion or specific events, detected and addressed after the fact. Integrating systems allows patterns of risk to be understood and predicted, sequences of behavior to be studied, and the sphere of analysis to extend far beyond the event.

For data centers, where even minor disruption can lead to major consequences, the ability to identify early signals is invaluable. It supports a proactive operational model which bases intervention on insight as well as alarms. Those operating facilities are typically judged based on uptime, efficiency and predictability. Systems which can detect faster and alert to even the small things serve to boost those metrics.

Going beyond the human

For cameras to provide true operational efficiency, their sphere of detection should expand beyond the human boundary. Thermal cameras can monitor the heat of server racks, offering early alerts that feed directly into maintenance workflows. Audio analytics can identify anomalous sounds that indicate equipment wear before failure occurs. External systems can track environmental changes that may affect operations. The point is not the individual capabilities of cameras and analytics, but the way these functions connect to the overall data center management structure.



> **"Security systems create a vital data layer. They should be treated as a core part of infrastructure, considered alongside power, cooling and connectivity at the earliest design stage."**

For architects and engineers, system behavior matters far more than feature lists. When security systems are treated as sensors and designed to be part of the operating environment from the outset, their data can be integrated, correlated and acted upon as part of day-to-day operations. Interoperability comes as standard. Introduced later, they are far more likely to remain standalone, their insight underused and their operational value diminished.

The other side of security

Deep integration increases exposure. The more security systems become embedded, the more the question of trust, and specifically of their cybersecurity credentials, is raised. With cameras and sensors sitting on the same infrastructure layer as mission-critical systems and DCIMs, a poorly-protected, compromised, or ill-maintained device could prove the ideal jumping-off point from which a digital intruder could move laterally into the heart of the network.

Just as the devices themselves must be designed into the network, their security must be designed into them: secure boot, key vaults, and supply chain audits are as crucial a component of a security device as the quality of its sensor.

Maintenance, both physical and of device firmware, is equally important. A camera or sensor cannot be forgotten about, it has to be cataloged, monitored, and updated in as streamlined a manner as possible. In many cases, today's cameras can assess their own output, using image health analytics to detect potential faults or changes and flag these automatically even before regular maintenance schedules are activated.

In practice, security is a primary consideration. It is fundamental to modern systems design. Approached as a priority, it strengthens both protection and performance. Tacked on, for all its benefits, it does not offer everything it could to the systems it was meant to support. Trust is designed in early, or it is difficult to establish at all.



From theater to resilience: lessons from the Nordic data center rulebook





Sienna Cacan, Global Enterprise Segment Marketing Manager, Axis Communications, explains why the Nordic data center market offers a useful model for treating security as a core part of the operating environment.



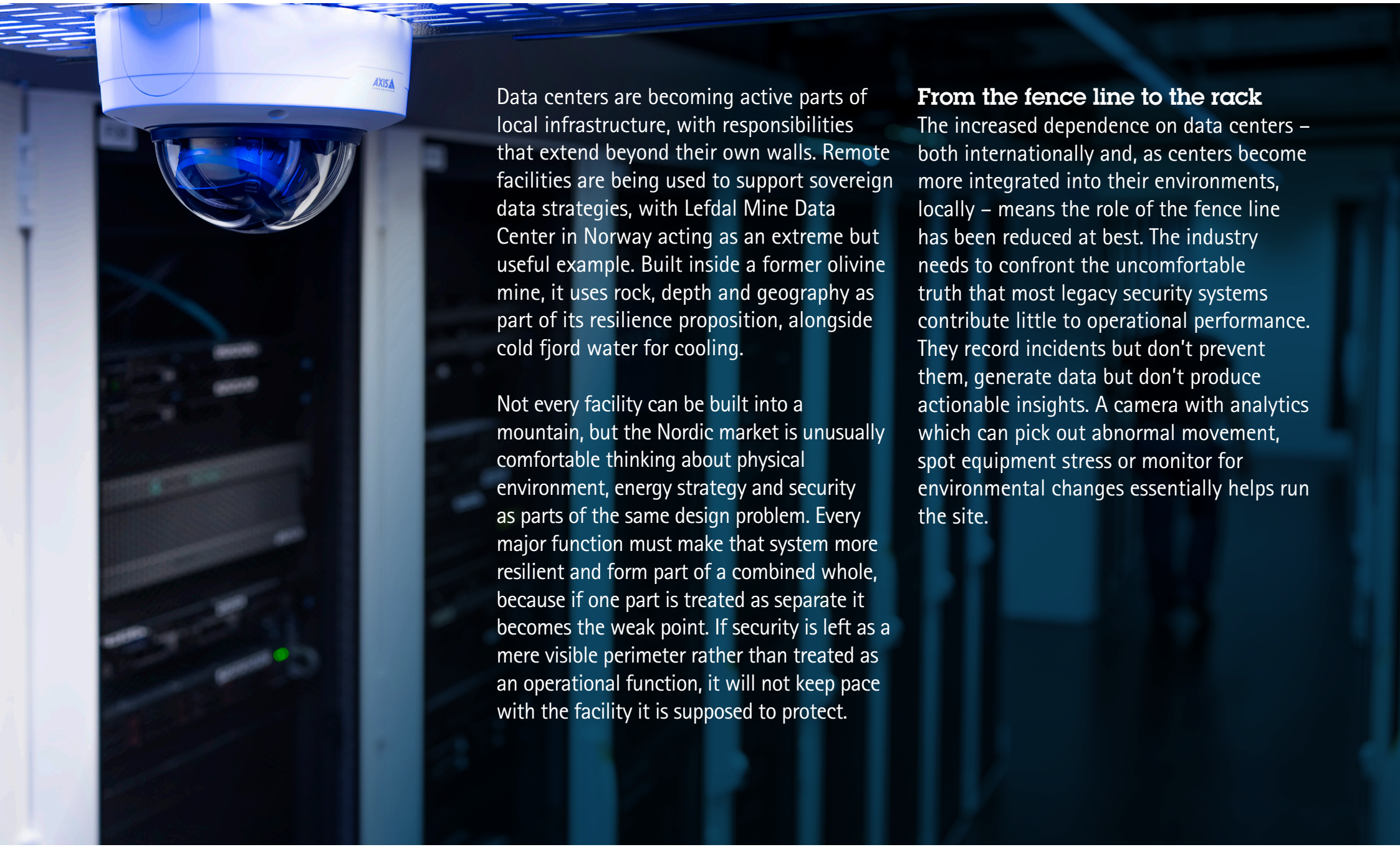
The data center has a security problem – and it's not what most operators think. Data centers excel at what almost amounts to theatrical security: the fences, cameras, access control systems and guards which surround the perimeter. These measures are necessary, but they create a false sense of completion, and the illusion of control. Modern facilities require a shift toward operational intelligence, where security systems actively contribute to uptime, efficiency, and risk mitigation.

Data centers are operationally complex models of critical infrastructure. They carry workloads that entire economies depend upon. AI compute, cloud expansion, and edge deployments are pushing facilities to operate at unparalleled scale and complexity. In this environment, the margin for error is nil. Security cannot, therefore, simply manifest as a layer built around a center's operations: it must be a core part of those operations, extending from fence to rack. The world is dependent on data centers getting it right.

The Nordic operating model

Across Sweden, Denmark, Norway, and Finland, a different model is emerging. The Nordic market has established itself as a global data center hub. It is an ideal habitat for data centers in general, offering renewable energy, cooler climates and political stability to an industry which needs all three. The key is that Nordic data centers operate with their environment, and not against it.

> *In Helsinki, for example, North's FIN02 facility has been designed to feed excess heat into the local district heating network, turning what would once have been treated as a cooling problem into a community energy resource. In Norway, Green Mountain has explored a different version of the same idea, working with seafood producers to use waste heat in land-based aquaculture.*



Data centers are becoming active parts of local infrastructure, with responsibilities that extend beyond their own walls. Remote facilities are being used to support sovereign data strategies, with Lefdal Mine Data Center in Norway acting as an extreme but useful example. Built inside a former olivine mine, it uses rock, depth and geography as part of its resilience proposition, alongside cold fjord water for cooling.

Not every facility can be built into a mountain, but the Nordic market is unusually comfortable thinking about physical environment, energy strategy and security as parts of the same design problem. Every major function must make that system more resilient and form part of a combined whole, because if one part is treated as separate it becomes the weak point. If security is left as a mere visible perimeter rather than treated as an operational function, it will not keep pace with the facility it is supposed to protect.

From the fence line to the rack

The increased dependence on data centers – both internationally and, as centers become more integrated into their environments, locally – means the role of the fence line has been reduced at best. The industry needs to confront the uncomfortable truth that most legacy security systems contribute little to operational performance. They record incidents but don't prevent them, generate data but don't produce actionable insights. A camera with analytics which can pick out abnormal movement, spot equipment stress or monitor for environmental changes essentially helps run the site.

There is a place for visible security. It shows that a facility has defenses and creates the appearance of control. But the interdependent Nordic approach teaches us that we must build security for the data center environment specifically and acknowledge that an effective security approach is one which considers the intersection between physical incidents, IT, and operational technology (OT). Video analytics and connected sensor platforms enable real-time, remote decision-making across distributed sites, an increasingly important capability as operators scale geographically.

A forced door in a data center can quickly become a cyber incident. A compromised connected device can be a route through the virtual perimeter and into the network. A cooling issue can become an availability event – or a threat to physical safety. Very different categories of incident, but they share a common outcome: disruption.

Security through connected signals

Operators need systems that connect signals rather than simply collect them. Video, access control, audio, environmental sensors and analytics all have value on their own, but their real strength comes when they contribute to a shared view of a facility. A single alert may mean very little. A door event, a record of unusual movement, a temperature change and an equipment alarm in combination may tell a different story.

This is where the region's interest in **digital twins and real-time facility models becomes relevant.** In a large or remote Nordic site, the useful view may not be a guard watching a flat wall of feeds, but an operational model based on a trusted sensor platform that brings video, sensors, access events and environmental data into the same frame. A failing door seal, abnormal rack vibration or unexpected movement pattern may each be minor in isolation. Together, they may point to an issue worth acting on before it becomes an outage.



This is what real resilience looks like: not stronger barriers, but visual verification, audit trails, SLA evidence and increased customer trust built through smarter integration and a willingness to rethink what security is actually about. As hyperscale and colocation facilities continue to expand, the industry needs to be honest with itself that security has often not evolved at the same pace as capacity, and scaling conventional security into larger, denser and more automated data centers does not automatically improve protection.

Building true resilience with integrated thinking

In truth, the next wave of data center disruptions is unlikely to result from inadequate perimeter defenses. Instead, it will stem from blind spots in operational visibility, delayed responses to emerging risks, and an overreliance on manual processes in increasingly automated environments. Essentially, it will come from treating security as a cost center rather than a strategic capability.

The lesson is not necessarily to copy the Nordics exactly, of course. Geography, energy markets, and local regulations differ. But copying the key lesson, that resilience comes from integration, is viable everywhere. As data centers become ever more critical to the global economy, the systems that protect them must also enable performance. If your security system doesn't improve uptime, it is already obsolete.

A data center that looks secure may still be fragile. A data center that understands itself, monitors its operations and connects security intelligence with operational decision-making is far harder to disrupt. Security should not sit around the data center; it should run through it. Anything less is theater, and that is a poor foundation for critical infrastructure.

“A data center that understands itself, monitors its operations and connects security intelligence with operational decision-making is far harder to disrupt.”

Back to contents ↑

Automated intelligence: closing the gap between the rounds



Peter Dempsey, Data Center Lead at Axis Communications, argues that as data centers grow larger and denser, periodic checks are insufficient – but the solution lies in finding context by connecting what's already there.

Data center operators already fully understand the pressures of maintaining uptime, resilience, and power and cooling demands. Faults can move quickly, and every intervention carries operational consequence. Regular inspection and maintenance are essential, but evidence gathering often does not keep pace with changing conditions within data center facilities.

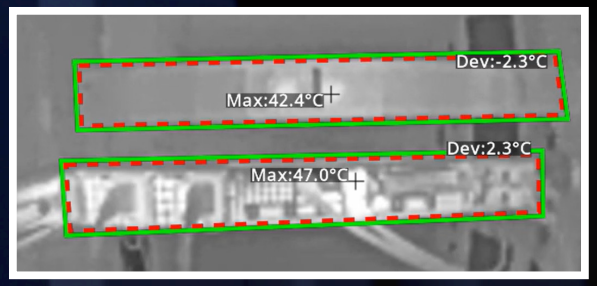
There is a better way: used as intelligent operational sensors, network cameras can complement intermittent observations with continuous evidence, helping teams verify faults sooner, target maintenance more accurately, and protect uptime without adding further rounds. On-device analytics can then identify faults at the edge, interconnecting with other safety systems to provide the kind of low-latency early warning that physical inspection cannot match.

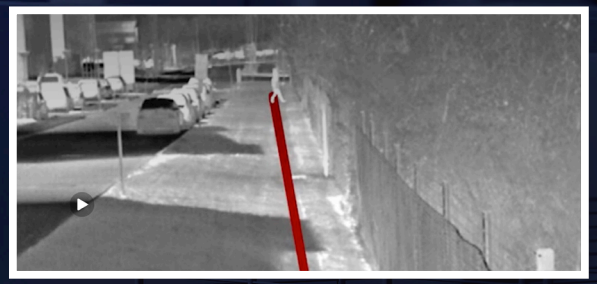
Inspecting a moment in time

For the small teams running large data centers, maintenance is bread-and-butter work. But inside many sites, important checks still depend on manual routines. An engineer walks gray and white spaces checking equipment with a thermal camera, or reads and logs a gauge. A plant room might be inspected on a regular schedule, or the status of a door checked as part of a guard tour. There is no question of discipline here, but 'doing the rounds' means the process is tied to a moment in time.

A scheduled check can confirm what was true at 10:15 AM, but it knows nothing of what began to change at 10:20 AM. If a battery string starts running hot between rounds, any resolution depends on another signal being raised or the next person arriving in time. If airflow degrades after maintenance work, the effect may build quietly before it becomes visible in the usual channels.







Shrinking the downtime margin

Data centers have become larger, and their racks denser. AI and high-performance workloads are changing the heat profile inside the hall. Liquid cooling is adding new environmental considerations. As power availability drives facilities into new regions, tolerance for slow detection is shrinking.

BMS and DCIM platforms remain the central systems of record for data center operations. Visual and thermal evidence gathering does not replace these, but it can enrich the information they provide by adding new physical context. Revealing the 'why' behind the 'what' helps operators decide whether an incident requires immediate attendance.

Early discovery for immediate resolution

Take a heat spike. It could point to a failing component. It could point to obstructed airflow after work at the rack. It could be a sensor fault, or the result of a condition that has already corrected itself. Physical evidence helps the operator distinguish between those possibilities, and automation has practical value when it turns repeated confirmation tasks into live operational data.

Sticking with heat, thermal rounds are the clearest example. A regular patrol with a thermal device looking for out-of-the-ordinary temperatures is useful work, but it is periodic; a fixed thermal view, though, gives much more immediate results. Any exception can be raised as it happens, accompanied by a view of the asset involved. If an area is running hot, the operator needs more than a number. They need to see where the issue sits and whether the response requires immediate attendance.



This same theory applies to processes like gauge monitoring. If a facility still depends on someone reading a gauge, taking a photograph or typing a value into a report, then the process is only partly digital.
A camera that reads the gauge and sends that value into the DCIM system turns a local indication into data that can be tracked, audited and acted on without waiting for the next inspection.

Building the technical bridge

This is where the technical bridge becomes essential. A camera, thermal device or audio sensor has limited operational value if its output stays in a separate interface. But through secure, open platforms which can support established protocols such as MQTT, Modbus TCP and OPC UA, they can be linked with the data already flowing through management platforms – giving a visual view to a BMS alert, or delivering that gauge reading directly to the DCIM.

That interoperability must preserve device integrity and protect communications throughout the system lifecycle.

The bridge also has to work in both directions. Camera and sensor data should be able to move into BMS and DCIM platforms and, at the same time, data from those platforms should be able to feed back into the visual layer to help create clear annotations of physical assets. If a smart rack is producing status information, that data can be associated with the rack being viewed. If a DCIM event relates to a specific cabinet, the operator can see the cabinet, the alert and the relevant condition in the same context.

This is about removing the visibility gap between a local condition and the operational system that needs to act on it. That connection can support workflows that raise work orders, escalate issues, or provide visual support to remote engineers. The data center sector has spent years building centralized platforms for management and control; integrating video and sensor data must boost these rather than replace them.

Evidence built for lean teams

Verification, checking, recording, and reporting will not, and should not, disappear completely, but skilled individuals should spend their time on decisions and intervention rather than the kind of repetitive evidence gathering that technology is made for. There is a commercial reality here as well. Data center teams are lean, yet facilities are growing and their need for operational evidence is growing with them. Adding more manual inspection is not scalable, but automation converts routine work into continuous and consistent feedback for the systems teams already trust.

In many cases the data center already has the systems and skilled personnel needed to measure and manage its environment. What it often lacks is a live connection between those systems and the physical reality they describe. This means the technical bridge should sit at the center of the operational evidence discussion. Without it, cameras remain cameras, sensors remain sensors, and management platforms continue to operate with limited physical context. With it, they unlock new value.

Once that connection works both ways, a threshold breach becomes a verified event, attached to the asset, visible in context and ready for a decision. Connected automation gives experienced teams better evidence, earlier.

“Automation converts routine work into continuous and consistent feedback for the systems teams already trust.”

Securing early: why data center resilience starts long before delivery





Axis Communications' Keith D'Sa argues that protecting scarce equipment between procurement and commissioning must form part of every data center's supply chain resilience strategy.



Ordering scarce equipment early buys developers time, but it comes with a security commitment that can run for months before installation even begins. A delivery may satisfy the procurement schedule while leaving expensive hardware sitting on a construction site before permanent protection is in place.

Protecting equipment between delivery and commissioning needs to be part of a developer's supply chain resilience plan, not an afterthought. Secure storage and a working response to unauthorized access should be in place before equipment arrives, as a condition of early delivery. Otherwise, the stock brought in to prevent one delay could become the cause of another.

Scarcity changes the calculation

This pressure is especially visible in the US, where AI infrastructure demand is driving rapid expansion. Globally, JLL's 2026 outlook puts average data center equipment lead times at 33 weeks – that's roughly 50% above pre-2020 levels.

Order too late, and a project can end up waiting for equipment it cannot do without.

Rising costs are compounding the problem. AI server demand has tightened memory supply and driven up its price, and simultaneously the price of copper hit record highs during 2026 . Expensive components and materials are attractive to thieves. Larger equipment may be harder to remove, but damage to a transformer or cooling system can derail a construction program just as effectively.

Developers are also dealing with local opposition to new facilities. Community objections should be engaged with on their merits. Separately, site risk assessments also need to account for deliberate disruption, including sabotage or arson, not just opportunistic theft.

The point is that losing equipment costs more than its replacement price. If a critical component cannot be replaced quickly, later work may need rescheduling and potentially push back the opening date. Insurance can cover the financial loss, but not conjure up an earlier delivery slot.

What happens after arrival?

Early deliveries can sit for months before installation. Some assets pass through an integrator's warehouse or a staging area; others are too large to move repeatedly without significant difficulty, and need to reach the construction site well ahead of when they're actually needed. Each transfer can change who has access and who is responsible for protecting the asset.

A delivery entry in a procurement system does not, by itself, establish what has happened around an asset since arrival, whether it has been tampered with, or whether it remains fit for installation.

A longer storage period extends the time during which equipment needs protection and its condition needs checking.

Physical assurance must, therefore, run alongside the paperwork. Developers should agree upfront who takes custody at each handover, how condition will be checked, who has access and who is responsible for investigating anything unusual. Ownership arrangements differ from project to project, so it's important not to assume that everyone knows who is actually watching the equipment.

Connected video and access control can give teams a record to investigate against between inspections. These systems complement receiving checks and physical inspection rather than replacing them. A camera cannot reliably establish what has happened inside a sealed enclosure.



Make an alert lead to action

Take, for example, equipment stored for a later construction phase. The area should theoretically be empty outside of scheduled access periods, but someone walks in and stays beside the equipment. Suitable video analytics can flag unexpected entry or loitering and trigger an alert, together with the relevant footage, for review by a security operations team.

From there, an operator can check the activity against authorised work and dispatch a guard if the operator assesses that one is required. Remote monitoring can cover this kind of incident before the data center even has an on-site operational security team. But this only works if the response is clearly defined, including who receives the alert and who has the authority to act.

As construction progresses, the site layout changes. Storage areas move, new materials block cameras, contractors show up at different times. That means detection zones, permissions and camera coverage need regular review as the work progresses. Protection designed around last month's site layout may no longer provide an adequate view of today's equipment.

Use the information beyond security

Site footage is not only useful for security. The same visual data can also support operational efficiency and business intelligence. A project team looking into a delayed equipment transfer, for instance, could cross-reference time-stamped footage with delivery records to pin down when unloading actually finished, and where the hold-up happened. If that delay keeps recurring, it is a signal to change scheduling or handling.



Thermal monitoring or smoke-detection analytics can flag developing conditions around stored equipment early enough to investigate before damage spreads. These applications still depend on suitable equipment and a defined response process. They do not replace fire protection.

Once the facility is operational, suitably positioned and specified cameras can continue protecting restricted areas while supporting day-to-day checks. Whether camera placement and system integrations will still serve the finished facility gives procurement a real basis for judging value beyond just the construction period.

Buy for the period of use

A system's total cost of ownership needs to reflect its full service life. A low acquisition price can quickly lose its appeal if early replacement, poor integration or disproportionate maintenance enter the calculation. Installation and ongoing support have a place in that comparison, as does cybersecurity; the support periods of cameras and access control systems must match the timespan that they will actually stay connected.

A trusted vendor should be able to explain its vulnerability-handling process and commit to clear software support periods. But the final responsibility still sits with the data center developer. They should settle, in advance, what the system must do from end to end, and determine who maintains the system once responsibility shifts from construction to operations.

Make the first equipment delivery both a security and logistics milestone in the construction program. Before it is authorised, secure sign-off from procurement and security on storage arrangements, handover responsibilities and response procedures. Test whether an alert can reach someone able to intervene. Build that work into the budget and program from day one, because if protection is not ready, neither is the site.

"Protecting equipment between delivery and commissioning needs to be part of a developer's supply chain resilience plan, not an afterthought."

Back to contents ↑

Why Axis: Driving cybersecurity

Axis is fully transparent in our vulnerability management. We use the Axis Security Notification Service to keep you updated on any issues around software and services connected to our technologies, and Axis Device Manager lets you remotely check that your technology is functioning correctly and that all software is up to date. We also offer guidance and training on how to implement best practices and processes. 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.





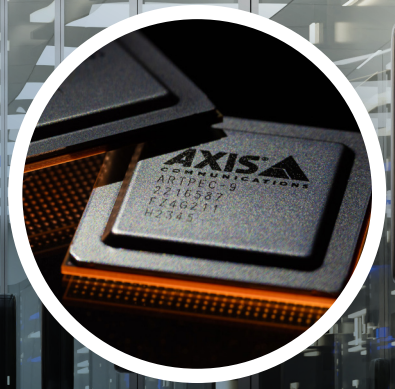
Quality in everything we do

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.



Get in touch with us!

Every data center has its own challenges, priorities and opportunities to build resilience. Whether you're planning a new facility, optimizing existing operations or exploring how smarter security can support uptime and efficiency, our experts are here to help you turn insight into action.

Contact us

Read more about Axis data centers

©2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC and VAPIX are registered trademarks of Axis AB in various jurisdictions. All other trademarks are the property of their respective owners.

AXIS COMMUNICATIONS