Data centers

Axis magazine, Issue 2

The AI effect and data centers:

supporting growth in digital infrastructure

Growing pains: the barriers to APAC's data center revolution

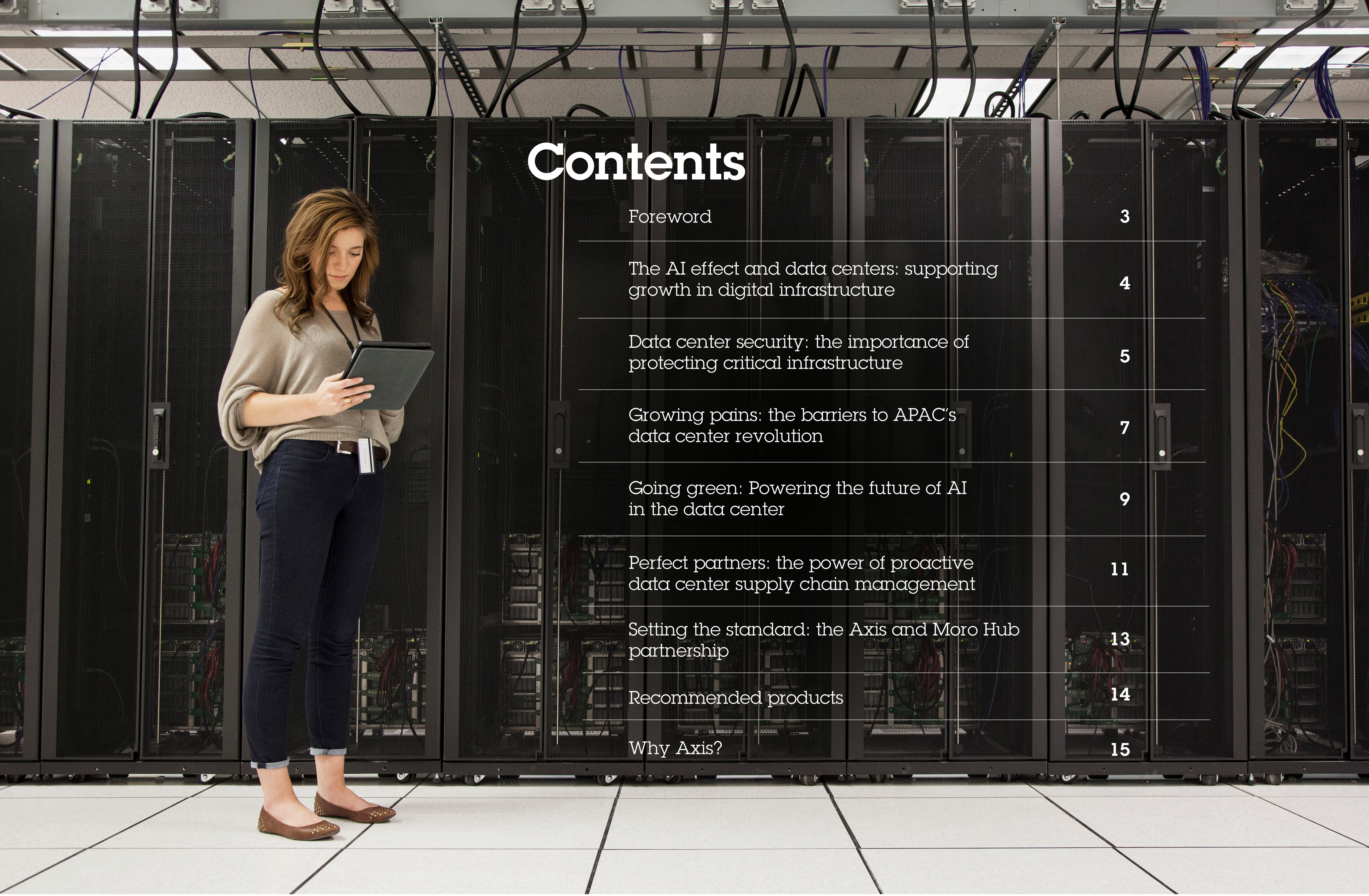
Data center security: the importance of protecting critical infrastructure

Perfect partners: the power of proactive data center supply chain management

and more!

Enter >

AXIS COMMUNICATIONS



Contents

In today's digitally driven world, data centers have evolved from being mere repositories of information into the beating heart of global innovation and connectivity. With the ever-increasing demand for real-time data, cloud computing, and edge technologies, the role of data centers has become more critical than ever. However, as we scale our infrastructure to meet these demands, we face complex challenges that require innovative solutions and strategic collaboration.

In this issue we are deep diving into the core topics shaping the future of the industry: **Security** – a non-negotiable priority with data breaches and cyberattacks becoming more sophisticated and frequent, security remains a top priority for data center operators. **Artificial intelligence** that is unlocking new possibilities, reshaping the data center landscape and driving innovation. **Operational efficienc**y is the lifeblood of a successful data center. In an industry where uptime is paramount and margins are tight, the ability to optimize every aspect of operations can make the difference between success and failure.

As the demand for data grows, so does the environmental impact of data centers. Energy consumption, water usage, and carbon emissions are all critical concerns for operators and regulators alike. But **sustainability** is not just a challenge – it's an opportunity to innovate and differentiate.

No data center operates in isolation. Success in this industry requires collaboration across a diverse **ecosystem of partners**, including technology vendors, service providers, and industry stakeholders. By working together, data centers can drive innovation, enhance service offerings, and build more resilient infrastructures.

A vision for the future

As the data center industry continues to evolve, **success will be defined by the ability to innovate, optimize, and collaborate.** Security, efficiency, AI, sustainability, and partnerships are no longer separate priorities – they are interconnected elements of a resilient, future-ready data center. We hope this issue provides valuable insights and inspiration as you navigate the path forward. By addressing these areas holistically, not only are we prepared to meet today's demands but also poised to shape a sustainable and secure digital future.

Sienna Cacan, Global Enterprise Marketing Manager

The AI effect and data centers: supporting growth in digital infrastructure

Sienna Cacan, Global Enterprise Segment Marketing Manager at Axis Communications, explores the potential of cutting-edge technology to make data centers smarter, safer, and more efficient.

The digital infrastructure sector is set for explosive growth. Demand for electronic services is likely to double over the next decade, and the worldwide data-center industry could triple* in size over the same period to meet this expanded need. Much of that infrastructure powers the day-to-day services that the world has come to rely on, but a huge part of the growth in demand comes from the next generation of service provision: the world of AI.

Artificial intelligence has changed significantly in recent years. Generative AI's many headlines have come from its rapid evolution, and we've seen text, image, and even video generation moving into mainstream tools. But predictive AI – built not to generate data but to analyse and draw conclusions from it – has received a more muted public reaction. This is despite its potential to extract valuable insights from sound, images and, most importantly, video beyond anything we could ever hope to achieve with humans alone.

Uniting video data and AI

AI is not just a growth driver, it's a growth enabler. As data centers expand in size and become more complex, and as their locations spread to meet demand across the globe, AI will play a vital role in simplifying the local and remote management of data center sites. As power draws increase – generative AI alone is expected to require an additional 38GW by 2028 – AI will help find new efficiencies and discover sources of waste. And as data centers enter their critical entity era, AI will support the essential security and safety function of sites.

Video data is now a rich resource for AI analysis. A camera is potentially the strongest sensor a business could employ, generating millions of data points multiple times every second. Every pixel can be isolated and analysed, a single camera view split into numerous points of interest to allow one camera to perform multiple jobs at once.

Object-based analytics can detect, track, and classify items within a scene, and trigger automated processes based on easily defined rules. Cameras are versatile, and their applications are almost limitless.

Existing technology, new opportunities

If a camera can see something, AI can act on it. Through deep learning, it is possible to develop custom reactive applications which offer new solutions to old problems, or spot new problems before it is too late to act upon them. And contrary to the heavy AI workloads which underpin the rapid growth of data centers, properly trained AI models allow such analytics applications to run directly on the network edge, within the very camera hardware they rely on.

That means a camera already in use for security could enhance its abilities, using AI analytics to identify unauthorised personnel in sensitive areas and automatically sounding the alarm, or detecting and alerting operators to suspicious activities like loitering or break-ins. But it also means that same camera could do more – it could integrate with an access control system to detect tailgating, or work in tandem with a thermal camera to offer operators a live view of any hot spots and even trigger additional cooling automatically.

Supporting the future of data centers

Data centers are the cornerstone of tomorrow's technology, but nobody is saying that the rapid expansion of digital infrastructure will be easy. Operators need every advantage they can get, be that saving money, saving energy, or just running facilities as cleanly, efficiently and safely as possible. AI analytics offer all of these advantages and more, all as an extension of hardware which would be required for the security function whether analytics were used or not.

*All facts and figures drawn from iMasons State of the Digital Infrastructure Industry report 2024.

DATA CENTER SECURITY

The importance of protecting critical infrastructure

Cyber attacks can come from anywhere and lurk undetected for years - says Peter Dempsey, Axis Communications - so it is imperative that data centers arm themselves with resilient security hardware to avoid breaching ever-more stringent regulations.

For cyber criminals, data centers represent a lucrative and attractive prize, whether the aim of the attack is to steal data, disrupt critical systems, or deploy ransomware. A data center represents a huge number of systems, processes and hardware devices, and a chink in the armour of any of these is all it takes. If it can be exploited, it will be – and there are many potential avenues of entry.

Over 20,000 Data Center Infrastructure Management (DCIM) systems have been found publicly exposed, and these could allow an attacker to disrupt a data center by altering temperature and humidity thresholds. Some UPS systems have also been found to be vulnerable, giving hackers access to data center power. And data centers are filled with Internet of Things (IoT) devices which could act as attack vectors. Data centers must be aware of their vulnerability and strive to protect every part of their infrastructure.

APT31 – Prepare for undercover attacks

Many data centers could already have been silently compromised. Attackers are increasingly deploying sophisticated 'living off the land' (LOTL) attacks which make use of the core tools of computer systems rather than installing their own malicious files. This kind of infiltration is difficult to spot, and indeed can stay undetected for years until the bad actor is ready to strike.[1]

These actors can be major entities. In many cases LOTL payloads originating from state-sponsored agents have been found lurking on critical networks. The NCSC has now implicated a state-sponsored hacking group, APT31, of attempting to target a group of MPs. In a list of other targets, the APT31 cyber-threat extends to the UK economy, critical national infrastructure and supply chains.[2]

This highlights the need for data center managers to take a proactive approach to security, one which does not simply lean on known cybersecurity principles but employs active monitoring and strict due diligence. And it is especially important in today's regulatory environment.

NIS2 – Detecting data anomalies in critical infrastructure

The NIS 2 Directive (NIS2) and the Cyber Resilience Act reclassify data centers as critical infrastructure. They now fall into the same category as healthcare, energy and transportation, and will meet the same level of scrutiny over their governance. Data center operators, whether under the jurisdiction of such legislation or not, have no choice but to tighten their defences.

The behaviour of every piece of hardware, software and firmware within a network must be regularly analysed in order to spot even the most innocuous-seeming unusual activity. This detective work must also extend beyond the bounds of the data center, because NIS2 applies to the activities of collaborators as well as critical entities. This includes equipment vendors and, crucially, every step in their supply chain.

Finding supply chain vulnerabilities

If an attacker cannot infiltrate a data center through direct means, it may attempt to inject a malicious payload on equipment which is yet to be deployed. IoT devices are fertile ground for criminals: they are network-attached by default and often not inspected with the same level of detail as more obvious attack vectors would be. As with LOTL payloads, malicious IoT devices may simply hide in plain sight because they allow attackers to piggyback on implicit trust.

Supply chain attacks are incredibly dangerous and growing, exceeding direct malware attacks by 40%[3] in 2022. There is no longer any way to justify any implicit trust: vendors must demonstrate the security and purity of their supply chain in detail and take action to ensure that unauthorised modifications do not happen. Data centers, in turn, must reevaluate every vendor relationship to ensure they are not caught out.

Thankfully modern technology allows suppliers to demonstrate the legitimacy of their hardware quite cleanly. Trusted platform module hardware protects signed firmware, offering confidence in a device's integrity along the chain. Secure boot prevents unauthorised firmware from running at all. And some devices can store cryptographic keys and certificates securely within, strengthening their security credentials while simplifying the process of managing one's defences.

Dealing with regulatory pressure

Regulations such as NIS2 basically offer data centers no choice but to act now or face massive fines. Their terms make data center directors liable not only for internal breaches but for those caused by some third-party security lapses. Security must be reevaluated from top to bottom.

Strong physical security through cameras, thermal and radar detection, and access control is clearly vital, because an attacker on site could cause untold disruption.

But logical security is just as vital to ensure attackers do not reach one's site virtually. Every piece of hardware and software, whether within the scope of the regulations or not, should be catalogued, analysed, prioritised, and documented on a regular basis.

Compliance needs to be substantiated with a clear record – and vendors must supply this too. No supplier of any value would wish to issue anything which is not on the level; working with vendors that care about their products is the path for data centers to create a smarter, safer world.

[1] www.silicon.co.uk/security/security-management/ncsc-warns-of-living-off-the-land-attacks-against-critical-infrastructure-549334
[2] www.news.sky.com/story/china-cyber-attacks-a-reminder-beijing-poses-constant-and-sophisticated-threat-to-western-cybersecurity-13101791
[3] www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/

Growing pains

The barriers to APAC's data center revolution

Anand Chandrashekara, APAC Relationship Manager at Axis Communications, argues that Asia Pacific is fertile ground for data center growth – but is not without its challenges.

The APAC region represents a shining investment opportunity for those wishing to get in on the ground floor, as it were, in the building of accelerated digitalisation. The Global South is a melting pot of new technologies – 5G deployments, smart city projects, medical advancements, an increasing reliance on AI, and a rise of general populous computing. These all make the region a highlight growth market, one which presents an increasing need for cloud services and data centers. APAC is set for great advances, but the region is not without its challenges if operators are to deliver that progress.

Energy supply and demand

Energy availability remains a barrier for data center expansion worldwide. Data center operators are aware of the steady growth in demand and the need to prioritise robust available supply above all else. Interestingly the APAC region leads the world in supply growth: between 2018 and 2023 the compound annual growth rate of data center live supply in APAC was 19.1%, compared to 16.7% for the Americas and 13.6% in EMEA.[1] But the level of desire for expansion in the APAC region is not yet matched by the pace of energy infrastructure growth.

In order to improve the volume and reliability of supply, developing nations facing economic disparity need the investment and commitment of data center operators. Conversely, operators need a consistent energy supply and the additional capacity to expand if required. Grids are hardening, and solar is steadily growing, but both demand money, time, and physical space. Certain APAC countries may even have reached their limit: Singapore had just 4MW of capacity to offer as of July 2023, and the highest energy lease fees in the world.[2]

Land and construction cost considerations

Growing utilisation of innovative technologies has created an exciting landscape, but the issue of limited capacity is equalled by the issue of land and construction costs. Moving data centers to more rural locations might be an obvious response, but land with suitable available power is scarce. What's more, raw materials, transport prices, and energy supply fees remain at an all-time high throughout the world, and construction costs have risen sharply to match.

Some data center businesses are waiting to invest in new locations until a market correction occurs, electing instead to expand existing operations. That is not to say that APAC's data center growth has stalled. China, Australia, India and Japan are rising fast in the world rankings.

[1] www.datacenterdynamics.com/en/news/apac-markets-experienced-largest-data-center-growth-between-2018-2023-dc-byte/
[2] www.cbre.com/insights/reports/global-data-center-trends-2023

But operations cannot be ring-fenced only into the most tech-forward nations, particularly given the volume of data protection and data sovereignty legislation enacted in the region over the past half decade, and those laws which are still to come.

Culture and character differences

APAC represents a broad spectrum of nations with little commonality and, in the case of areas like India, vast cultural and economic differences even within national borders. Demand for data is uneven, skewed by disproportionate wealth distribution; divisions of language and political trust can create barriers which delay harmonious development; potentially volatile areas of the region add uncertainty, complexity and ambiguity which can hamper enthusiasm for investment.

This is true of large-scale data center development and is also true down the chain. There is growing concern surrounding the tech used by data centers in low-income countries, and its selection based on price rather than performance. Data centers cannot be part of a race to the bottom, because the potential impact of data breaches or unavailability are massive. Operators must select hardware throughout the data center which puts reliability and cybersecurity first, no matter the cost.

Working with proven technology

Basic cost/benefit analysis is not enough for data centres eager to push what are often difficult limits of power and bandwidth. They must search for truth.
Proof of concept – actual, tangible proof – must be considered a vital component of product selection. Whether this comes from data sheets featuring accurate metrics or a robust programme of first-hand testing, it is both up to vendors to supply data centre operators with technology which demonstrably meets their needs, and also on operators to select their vendors on this basis.

Given the importance of regulatory compliance and a robust digital architecture which keeps customer data safe, security is a prime factor. With the cybersecurity landscape constantly changing, only devices which consistently harden their defences through upgrades, updates and testing will suffice – and vendors must demonstrate a security-first approach by embracing encrypted communications and secure, signed firmware.

APAC's continued growth requires investment, drive, and a cautious approach to risk management. Many parts of the puzzle are held by national governments, and will only be solved with time, investment and significant public and private pressure. But a large part of the risk factor can be mitigated if operators use technology that is fit for purpose. A smarter, safer world is built on hardware which is secure by default, and which works as it should – not as it merely claims.

Going green

Powering the future of AI in the data center

AI's speed to market has been incredibly fast, and it's growing even faster. Generative AI is becoming understood, widely used, and its complexity and computing demand is rapidly expanding.

Joe Morgan, Business Development Manager for Critical Infrastructure, Americas, at Axis Communications, explores the power that data centers hold to change the way theworld thinks about energy and sustainability in the AI era.

The US leads the world in data center numbers, housing over 5,300 as of March 2024[1], but this growth will see data center demand double or triple in the very short term. Inside the server room and out, the data center industry is now stretching to meet demand.

The rapid expansion of digital infrastructure is, on the surface, at odds with green initiatives. AI needs power, and lots of it. This puts broad constraints on data center locations, which require ready connectivity to an adequate supply, and US provision of renewable energy is lacking – only 9% of energy use in 2023 came from sustainable sources.[2] The American data center industry has no choice but to navigate its journey of expansion in a sustainable and responsible way from top to bottom, but it is clear that it will not be easy.

Sustainability, four ways

Outside of energy requirements, data center companies need to consider four key pillars of sustainability when creating new sites or upgrading existing facilities: these being physical security; operational efficiencies; disaster resistance; and cybersecurity. None of these can be ignored, and all offer opportunities to act in a more sustainable manner.

The problem is that the industry is necessarily working fast. Implementing fresh solutions to these pillars while attempting to maintain sustainable principles is difficult enough, but they must also be the correct solutions. The pace of data center expansion means it is all too easy to overlook the obvious. You can be sustainable, but you must also be clever, and an intelligent choice of technology is vital.

The importance of ingenuity

Take security, for instance. A simple switch to high-quality thermal, infra-red and low-light cameras can help deal with security concerns at night, while removing the need for additional lighting and improving the operational efficiency of a data center. But that is only their most simplistic use case. Cameras can do so much more than stream video. They are the most powerful sensors a site has, picking up millions of data points every second.

Just as the world's use of AI expands, so can AI use within the data center. The same camera that powers the security function can monitor the people on site. It might use AI-based techniques to detect if proper PPE is being worn, see if an employee has fallen, tie in with access control systems to help count staff in the case of an evacuation, or even alert to loitering in restricted areas.

One sensor, many uses

Within the server room cameras can protect entire racks, acting as a vital visual indicator for overheating, detecting smoke or fire, and working with other sensors to assist with more complex operations like cooling adjustments. And the right cameras, built with cybersecurity principles from end to end, offer operators assurance that they cannot be used as a convenient IoT tunnel into a data center's wider network.

These functions only skim the surface of what a single sensor can do today, and it is certain that more efficiency and functionality will be discovered as data center sites evolve. These sensors are the backbone of internal change, and can help in a small way to reduce data center power use, but they are a drop in the ocean. Only a massive increase in the availability of sustainable power will guarantee the future of digital infrastructure.

Barriers to overcome

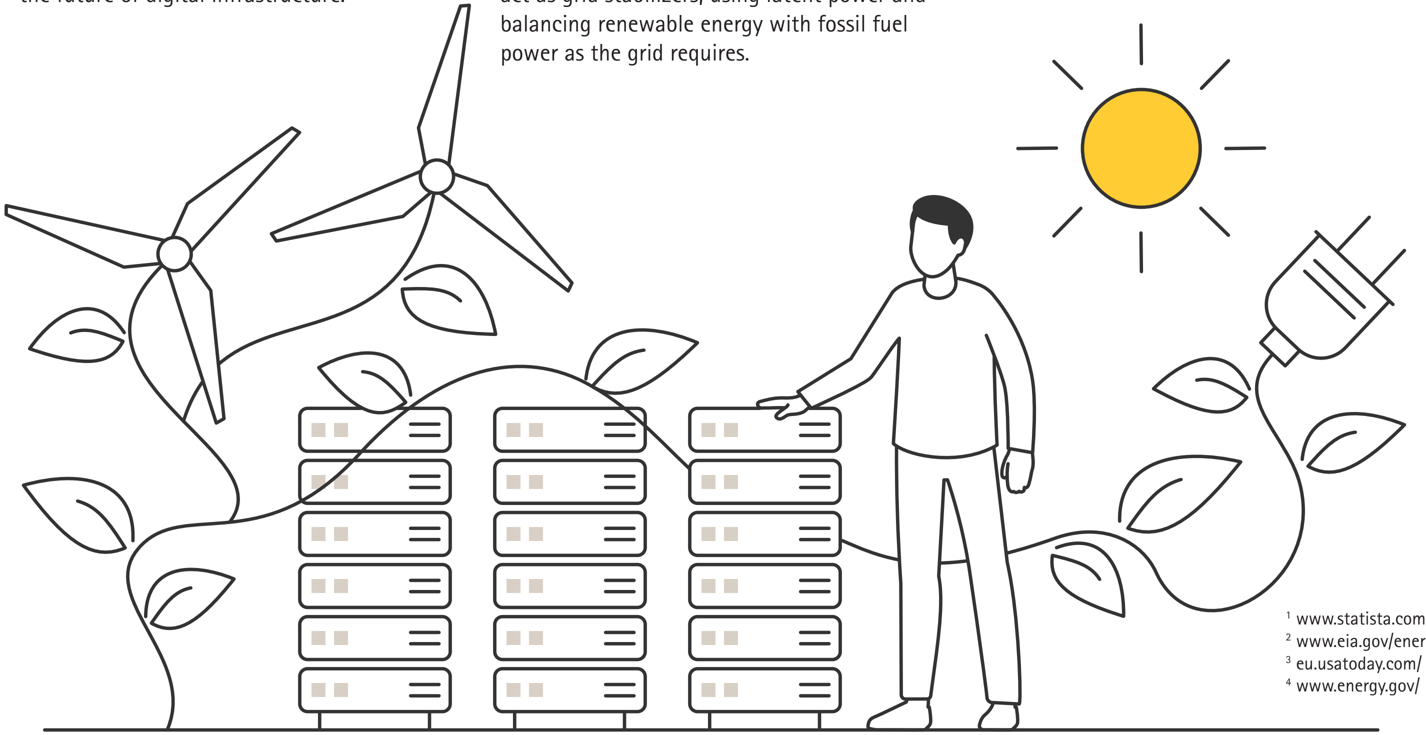
Renewables are not yet popular with the public. In contrast to the rapid expansion of data centers, the US saw twice as many solar and wind installations blocked as were built over the past decade.[3] This is despite the US Department of Energy's target of reaching 100% carbon pollution-free energy by 2035.[4] In contrast to many European nations, the Americas are far behind the renewable curve.

The good news is that the power consumption of data centers puts operators in a powerful position as the driving force of sustainable energy solutions. Some data center sites have developed their own solar and wind stations, often in very remote areas, enabled by remote monitoring and administration. Operators have invested in green energy power purchase agreements (PPAs), helping to grow the renewable industry. Data centers can even act as grid stabilizers, using latent power and balancing renewable energy with fossil fuel power as the grid requires.

The green power magnet

The key, though, is that data centers will always prioritize power availability. There is worldwide competition for countries to become the most skilled and capable providers of AI technology, making geography mostly irrelevant. Operators hold a powerful lobbying position because data centers will line up to purchase green power if it is available – in the Americas or elsewhere.

Those countries, states, and cities which prioritize renewables and go beyond global targets are those that will thrive in this new AI economy. And while data center providers focus on the big picture outside of the server room, they can lean on smarter, safer sustainability solutions within their walls in order to stay secure without worry.



[1] www.statista.com/statistics/
[2] www.eia.gov/energyexplained/us-energy-facts/
[3] eu.usatoday.com/
[4] www.energy.gov/

Perfect partners

The power of proactive data center supply chain management

wesco | anixter

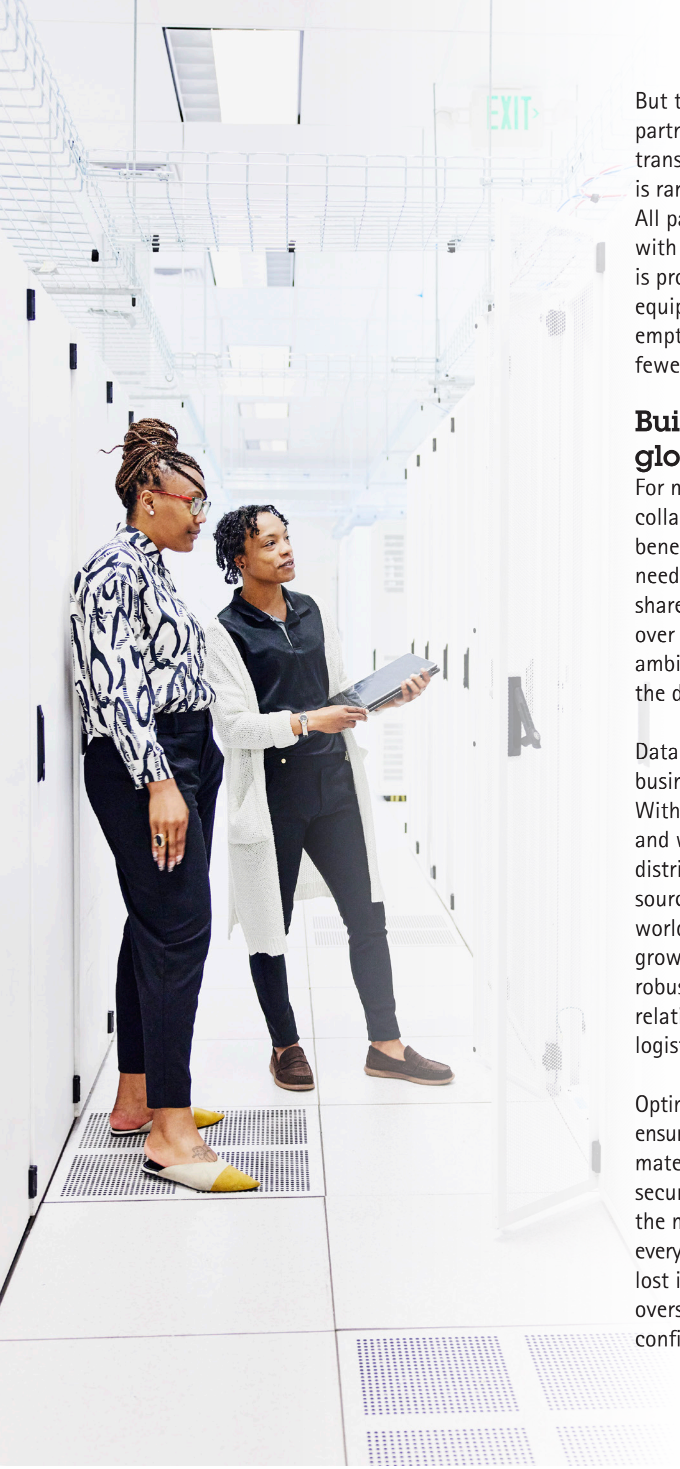
Aleksey Mayorov, Distribution Account Manager EMEA at Axis Communications, explains the importance and key benefits of close collaboration with distribution, and the steps data center operators must take to ensure timely access to critical resources.

In the fast-paced world of data centers, facilities need to be brought online quickly and efficiently – even the smallest delays can lead to significant setbacks and huge costs. Accenture reports that the world's low resiliency to delays, shortages and other market fluctuations costs $1.6 trillion in potential revenue growth every year.[1]

The risks of, for example, environmental regulation and geopolitical disruption, which 70% of operators suggest will limit digitalisation in Europe in the coming years[2], have to be mitigated. To do so, data center operators must nurture proactive partnerships with distributors that can offer reliable, scalable, and responsive service – those which deeply understand the unique, specific pressures affecting one of the world's fastest-growing sectors

A baseline standard for partnership

A proactive approach to supply chain management begins even before selecting one's partners and continues as those partnerships evolve. To begin with, data center operators should be looking up their supply chains for the 3 R's: Resiliency, Robustness and Responsibility. Resiliency represents the shield, there to protect against difficult times; robustness is the ability to act quickly if something does go wrong; and responsibility is a commitment to the highest quality, sustainability, and trust.



But trust is earned, not given – and in supply chain partnerships, trust is built on a foundation of transparent communication and commitment. There is rarely any wiggle room for delays or mistakes. All parties need to be on the same page, clear with their requirements and able to deliver what is promised. Clarity around project goals ensures equipment availability far in advance, thus a pre-emptive approach to trusted partnership leads to far fewer delays.

Building and growing on a global scale with Wesco Anixter

For many years we have worked in close collaboration with Wesco, developing our mutually beneficial and successful partnership serving the needs of our customers globally. The platform of shared values and trust that we have has matured over time and allows us to continue setting ambitious goals to meet the evolving challenges of the data center industry.

Data centers operate globally – and global businesses want to work with global companies. With an increasing number sited in remote regions, and with the technology market now so widely distributed, virtually every data center needs to source equipment and materials from all over the world. As data center projects expand to meet growing demand, it is vital that operators seek robust distribution partners which exhibit close relationships with their own manufacturers and logistics providers.

Optimising the supply chain is crucial in order to ensure timely access to critical resources. Construction materials, IT and energy infrastructure, physical security and access control systems – if just one of the myriad elements of a data center falls behind, everything falls behind. Consider the potential revenue lost if crucial equipment or materials are trapped overseas for weeks or months. Operators must be confident that their suppliers can deliver.

Disasters or global instability can be problematic, but distributors that are closely integrated with their manufacturers can, if looking far enough into the future, work through them. Operators, similarly, should consider their options: creating local partnerships or diversifying suppliers helps build a backup plan. A pre-emptive approach to dealing with issues can help operators, distributors and manufacturers alike develop a relationship built to encourage stability.

Alignment and efficiency through communication

A proactive supply chain strategy helps meet the precision challenge of worldwide procurement. If a supply chain partner is aware of deadlines and expectations far in advance, they can prepare. And when it comes to navigating the challenges of distance, it is far more straightforward to coordinate inventory, shipping, on-site logistics and cross-border complexities when close partnerships are built on transparent communication.

The best partnerships tend to be those made with mature and well-established distributors, whose infrastructure and expertise in planning ensure they can work with their manufacturers and logistics partners on an integrated approach to risk management and disruption prevention.

Integration doesn't stop there; shared understanding, supported by collaborative platforms, means data centers can make partners at all stages of the supply chain clear on the route forward and affect a quicker turnaround.

Every part of the supply chain provides a building block vital for the efficient completion and onboarding of data centers, and every partner should be treated with the same amount of care and clarity.

Working together with trust andshared values

In the end, any relationship with key partners comes down to trust – and while execution and communication contribute to building a shared culture, operators should be aligned with their distribution partners in terms of their values. Data centers need to meet the highest standards of cybersecurity and sustainability, and their equipment must play its part.

Partners with aligned values can help reinforce these standards. The supply chain is not only a source of equipment, after all; build trusted partnerships and it can also be a source of reassurance around secure handling and eco-friendly activities. That is, as long as distribution partners can offer straightforward, detailed and provable information on their manufacturers' sustainability and ethics practices.

The supply chain exists for a reason. No business can work alone. The role of a proactive, collaborative supply chain underscores the value of selecting partners who prioritize trust, responsibility, and forward-thinking solutions. By working together, data centers and their partners can create a smarter, safer environment on a global scale.

[1] www.accenture.com/content/dam/accenture/final/capabilities/cross-service-group/iconic-thought-leadership/document/Resiliency-in-the-making-report.pdf
[2] www.rlbinsights.com/reports/data-center-trends-report-2024/key-findings

Setting the standard

The Axis and Moro Hub partnership

As one of the Middle East's leading data centers, Moro Hub has both a desire and an obligation to ensure its premises are thoroughly secure. The Dubai facility is also committed to operating sustainability, as demonstrated by its innovative design and its use of renewable energy – it holds the Guinness World Record as the largest solar-powered data center in the world.

Since 2018, Moro Hub has partnered with Axis for its security needs. Axis visual and thermal cameras are installed throughout the facility, but most importantly they are integrated into a holistic platform. In fact, it's an excellent example of our five layers of protection in action.

It starts just outside the facility perimeter where Axis cameras are integrated with road blockers, under-vehicle scanners and loudspeakers to detect, verify, and deter unauthorized access. Analytics enable automatically triggered alerts, so personnel can be proactive about identifying and mitigating potential threats before they escalate.

The second layer of protection has surveillance cameras providing total coverage of the grounds and providing real-time information to both controllers and on-the-ground personnel.

The third layer controls entry to the main building. There, the access control system incorporates keycards, biometric scanners, X-ray machines, and a visitor management system to ensure that only people with the appropriate clearance level are allowed to enter.

Individual server rooms are protected by layer four. Motion sensors and fingerprint scanners prevent unauthorized access and keep a record of who is in every room and when.

Finally, the fifth layer protects individual racks with modular camera systems ensuring that sensitive data remains secure.

Moro Hub is a benchmark for data centers across the Middle East, so it is fitting that they have a comprehensive security solution in place. Crucially, they don't stand still. In partnership with Axis, they have implemented a system that can be scaled up and enhanced if required and when future innovations emerge. As well as optimal security, it's a system that reduces the need for manned patrols and uses metadata to provide operational efficiency insights – and it's set up to become even more impressive in the future.

> "As a valued partner, Axis is not just supplying us with a product. We are always looking for aftersales support and consultation, and how we can upgrade the existing system to align with the latest technology in the market."
>
> Ayman Alkhzaimi, Facility Manager, Moro Hub.

[See the full story here]

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 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.

AXIS P1245 Mk II Modular Standard Camera

Ideal for mounting in tight spaces, AXIS P1245 Mk II features a small, thumb-sized sensor unit that's easy to install and blends into any indoor environment. Featuring a deep learning processing unit, it enables the use of advanced analytics.

Axis PTZ cameras

PTZ cameras deliver real-time monitoring for wide areas thanks to pan, tilt, and zoom functionality. AXIS Q63 Series includes heavy-duty cameras that stand up to all weather conditions, and provides quick zoom and laser focus, even in the dark. With speed dry functionality, you get clear, crisp images even in rainy weather.

AXIS Q1961-TE Thermal Camera

This halogen-free, thermometric camera lets you remotely monitor temperatures and trigger temperature-based events. Ideal for improving operational efficiency. Robust and impact-resistant, it offers early fire detection analytics and built-in cybersecurity features.

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).

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.

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

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 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.