

IN DEPTH:
IT outsourcing
p7-8

The frontline isn't forgiving

Neither should your communications be

Alasdair Ambroziak,
Thales UK, p11



Driving DC sustainability

With the power of predictive artificial intelligence

David Pownall, Schneider Electric UK&I, p14



Questions and answers

Don't ask others for anything you wouldn't do yourself

George Ashwin,
AddOn Networks, p16



From Trump to tech: UK attracts massive US investment in AI hub



Following President Donald Trump's recent visit to the UK, the government has secured **£150 billion of US investment as part of a 'Tech Prosperity Deal' which includes a £90 billion pledge from Blackstone.**

The newly announced AI Growth Zone in Northeast England, with sites in Blyth and Cobalt Park, will leverage the region's abundant renewable energy resources and proximity to low carbon infrastructure. The sites will host major new computing infrastructure, including the rollout of up to 8,000 GPUs initially, scaling towards 31,000 under the Stargate UK plan from OpenAI, NVIDIA and Nscale.

In support of the move, Kevin McGuinness, Head of EMEA for Napier AI, shares that, "beyond the benefits that businesses have come to expect, the significant AI investment can also save the UK economy billions each year when deployed in high-impact areas such as financial crime prevention. UK financial institutions could save £2.2 billion annually through AI-driven AML solutions, while the UK could rescue £90 billion from financial criminals each year by using more effective AI."

However, for this £150 billion investment to deliver lasting impact, we need more than just

capital, notes Chris Davison, CEO of NavLive: "startups need access to strong infrastructure, reliable data pipelines, and environments where they can experiment and iterate safely. When these building blocks are in place, startups can drive real breakthroughs, by bringing AI tools that are not just novel, but trustworthy, scalable, and genuinely useful to businesses and society."

Lee Myall, CEO, Neos Networks, observes that while compute and power rightly capture headlines, fibre remains the missing piece in the UK's sovereign AI strategy. Without high-capacity, resilient fibre connecting these sites to businesses, data centres, and international networks, the full potential of these investments will not be realised.

"The UK has a once-in-a-generation opportunity to build data centre capacity that not only keeps pace with AI but strengthens our national resilience and competitiveness. To achieve this, we must match ambition in data centre build-out with ambition in connectivity - long-haul fibre routes, regional access and diverse corridors that enable the investment, and spread the benefits of growth beyond major hubs," says Myall. "If the UK is to lead in AI and digital infrastructure, fibre investment cannot be

an afterthought."

"We see first-hand how fragile progress can be when infrastructure isn't maintained or when expertise gaps slow adoption," agrees Claire Hu Weber, Vice President of International Markets, Fluke Corporation. "The UK must pair investment with practical support for apprenticeships, standards, and hands-on technology. That's where durable growth will come from, not just from billions pledged, but from ensuring the systems and people behind them can perform under real-world conditions."

Further, some critics have raised concerns over whether the benefits will be broadly felt across the UK's tech ecosystem or concentrated among a handful of foreign giants.

"It's particularly great to see British organisations Nscale and techUK so heavily involved - but the majority of those named in these projects at present are US based. British businesses and policymakers must make sure that UK companies are benefitting as much as American companies," says Allan Kaye, co-founder and Director of Vespertec. "It's vital that we work with our US partners on an equal footing to build up British AI, rather than just becoming more real estate for American data centres." ■



0800 978 8988

Powering Resilience since 2009

For 16 years, we've delivered trusted backup power solutions — ensuring uptime, continuity, and peace of mind for critical operations.

sales@criticalpowersupplies.co.uk | www.criticalpowersupplies.co.uk

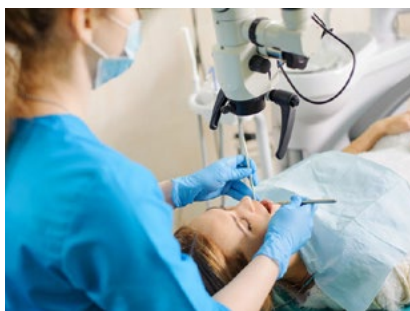
Wildix and RoboReception transform dental communications

A joint AI initiative between Wildix and RoboReception has yielded substantial improvements in patient access and operational efficiency across 65 dental practices in the UK.

Since its deployment in May 2025, the clinician-designed, 24/7 AI receptionist system has handled over 50,000 patient calls without a single missed contact, marking a significant stride in reducing missed calls — a challenge that has long plagued healthcare providers. Previously, up to one-third of new patient calls went unanswered, often resulting in lost opportunities and diminished patient care.

The innovative system has helped recover approximately £9 million in care revenue within just a few months of operation and has freed over 2,000 staff hours, allowing dental teams to focus more on clinical duties. This success is attributed to the voice automation technology that underpins the platform, which seamlessly integrates Wildix's Unified Communications as a Service (UCaaS) platform, powered by Wilma AI, with RoboReception's dentist-developed workflows. This integration provides practice staff with oversight on when AI should handle calls, when human intervention is necessary, and how call records are managed, with a smooth escalation process to live staff when needed.

RoboReception was founded specifically to address front-desk challenges faced by clinicians, with Co-Founder Dr Grant McAree emphasizing the importance of building a system that empowers clinicians rather than replacing them. He highlighted that the platform was created by clinicians for clinicians to give practices back control and improve patient access. Since launch, the system has managed to resolve 96% of calls autonomously, with only 4% requiring escalation to human staff. Monthly new patient bookings have increased



significantly from 18% to 70%, with an average of 500 new bookings per month and late cancellations decreasing by 75%.

The system operates in strict compliance with GDPR, ensuring encrypted communications, role-based access, and audit logs, addressing security and data privacy concerns. Industry leaders have praised the solution for its rapid deployment and clinician-centric approach. Dimitri Osler, Chief Innovation Officer at Wildix, noted that the technology is not only safe and trusted but also scalable, with practices expanding to hundreds of sites in a matter of weeks — a testament to the system's effectiveness and ease of integration.

The platform's comprehensive features also include real-time appointment scheduling, call transfers, and integration with existing patient record and CRM systems, facilitated by Wildix's open APIs and engineering support. This has enabled a rapid and seamless adoption across practices, surpassing traditional healthcare technology deployment speeds.

Building on this success, Wildix and RoboReception plan to extend the rollout to more than 500 practices across markets including Ireland and Australia. The expansion aligns with Wildix's strategic focus on AI-enabled unified communications that support operational growth in healthcare and beyond, promising to further enhance patient access and practice efficiency worldwide. ■

UK Data (Use and Access) Act 2025 promises clarity and revenue boost for retailers

The UK Data (Use and Access) Act 2025 (DUA) has been enacted to provide greater clarity for businesses regarding the lawful use of customer data, particularly around the concept of 'legitimate interest.'

This legislative change is expected to significantly impact marketing strategies and customer engagement within the retail sector, with projections indicating a potential uplift in retailer revenues.

The new legislation will lead to amendments in existing regulations such as the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR), which will be clarified over the coming year. These updates aim to offer retailers and organisations clearer guidance on how they can legally use customer and prospect data for direct marketing activities, reducing previous uncertainties that hampered data-driven campaigns.

Industry analysts from Sagacity estimate that UK retailers could see their revenues increase by at least 2%, translating to

approximately GBP £10 billion annually. This projection is based on the potential for increased data utilisation to drive sales. However, they cautioned that businesses must adapt their data management practices — such as maintaining clear audit trails and obtaining proper permissions — to fully capitalise on these opportunities and avoid hefty penalties. Under the new law, penalties for breaches of PECR are expected to align with those of the UK GDPR, reaching up to GBP £17.5 million or 4% of global annual turnover.

The act also emphasises stricter respect for customer preferences, making the creation of clear permission records and honouring opt-out requests more critical than ever. Maintaining accurate, comprehensive data trails will be essential for compliance and for leveraging new data-driven marketing opportunities. Additionally, the DUA introduces a 'recognised legitimate interests' basis for processing personal data, which simplifies compliance by removing the need to balance individual rights against business benefits in certain cases. ■

Latos secures approval for £100 million AI DC in Stockton-on-Tees

Latos has received planning approval to develop a new GBP £100 million data centre in Stockton-on-Tees, with completion slated for 2027.

Situated on a 1,750-square-metre site at Preston Farm Industrial Estate, the facility is tailored to support artificial intelligence computing at what is termed the 'neural edge.' This approach involves establishing smaller, distributed data centres closer to end users, aiming to reduce latency and enhance data-intensive applications such as robotics, autonomous vehicles, and real-time AI systems.

The Stockton site will feature two data halls equipped with Nvidia Blackwell GPUs, a cutting-edge technology optimised for large language models and computer vision tasks. Latos envisions this data centre playing a vital role in boosting local employment and stimulating the digital economy in the Tees Valley region, aligning with its broader five-year plan to develop a total of 40 'neural edge' data centres across the UK by 2030. Future locations include major cities such as Manchester, Birmingham, Leeds, and Glasgow, with the goal of ensuring that no part of Britain is more than 50 miles from an ultra-low latency AI service point.

Unlike traditional, large centralised data centres, Latos's 'neural edge' model aims to bring AI processing closer to users, enabling advanced applications in augmented reality, smart manufacturing, and predictive healthcare. Andy Collin, Managing Director of Latos Data Centres, explained that real-time AI applications like robotics and autonomous transportation require new infrastructure capable of handling demanding workloads efficiently. He highlighted that the neural

edge design is more energy-efficient, faster to build, and more cost-effective than conventional data centres.

The Stockton facility will be part of a distributed intelligence network that connects to additional sites planned across the country. It will support AI inference tasks in milliseconds, facilitating more sophisticated real-time AI processes and reducing dependence on centralised cloud processing. A key aspect of the project is its commitment to sovereign data processing, ensuring that data remains within the UK, addressing security and compliance concerns.

Latos pointed out that the Tees Valley region is experiencing rapid growth in its technology and digital sectors, making it an ideal location for this initiative. The area is the fastest-growing in the UK for start-up activity and hosts numerous manufacturing and engineering firms, as well as the government-backed Centre for Process Innovation (CPI). The company expects strong local demand for its services as regional development continues.

As part of its nationwide strategy, Latos plans to build a network of 40 modular, standardised AI processing facilities, designed to be quick to construct and cost-efficient. The company has already announced a 50,400-square-metre hyperscale facility in Cardiff, forming part of its broader rollout aimed at transforming the UK's AI infrastructure away from traditional cloud models. Collin concluded that this neural edge network represents a fundamental shift that will allow British companies to innovate and thrive using AI technology, rather than relying on outdated centralised systems. ■



EDITORIAL:

Editor: Amy Saunders

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Kevin Curran, Scott Baxter, James Griffin, Alasdair Ambrozak, David Pownall, George Ashwin, Lauri Salmia, Mark Klarzynski

ADVERTISING & PRODUCTION:

Sales: Kathy Moynihan
kathym@kadiumpublishing.com

Production: Karen Bailey
karenb@kadiumpublishing.com

Publishing director:
Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Image Court, IC13, 328/334
Molesey Road, Hersham, Surrey, KT12 3LT
Tel: +44 (0) 1932 886 537

© 2025 Kadium Ltd. All rights reserved.
The contents of the magazine may not be reproduced in part or whole, or stored in electronic form, without the prior written consent of the publisher. The views expressed in this magazine are not necessarily those shared by the editor or the publisher.

ISSN: 2052-7373

Gcore reveals surge in DDoS attacks and target sector shift

Ahead of Cyber Security Awareness Month (October), Gcore has unveiled its Q1-Q2 2025 Radar report, highlighting a significant increase in Distributed Denial of Service (DDoS) attack activity worldwide. The report underscores the growing sophistication and scale of cyber threats, emphasising the urgent need for organisations to strengthen their cybersecurity defenses.

According to the report, the total number of DDoS attacks in the first half of 2025 surged by 41% compared to the same period last year, totalling over 1.17 million attacks. Peak attack bandwidth also reached new heights, surpassing 2.2Tbps, exceeding the previous record of 2Tbps set in late 2024. The nature of

these attacks is evolving; while shorter attacks under 10 minutes have decreased by approximately 33%, there has been a near fourfold increase in attacks lasting between 10 and 30 minutes. These longer-lasting assaults are designed to bypass auto-mitigation systems and cause more extensive damage.

The report notes a shift in targeted sectors, with the technology industry overtaking gaming as the most frequently attacked sector. Financial services also experienced a 15% rise in attack volume, indicating that threat actors are increasingly focusing on industries that offer higher disruption potential and may have comparatively lower levels of cybersecurity preparedness.

In addition, application layer attacks — those targeting web applications and APIs — have become more prevalent, rising from 28% to 38%. This trend reflects a strategic move by attackers toward multi-vector assaults that exploit vulnerabilities in customer-facing systems. The largest recorded attack peaked at 2.2Tbps, illustrating the ongoing trend of unprecedented attack sizes and scales.

Attackers are increasingly adopting multi-vector tactics, embedding malicious traffic within legitimate-looking streams to evade detection. The rise in longer-lasting attacks appears to be a deliberate attempt to test infrastructure resilience and maximise disruption. Hosting providers, supporting services such as

SaaS, e-commerce, gaming, and finance, have become prime targets, as attacks on these entities can cascade into widespread outages and damage their reputations. ■



DHSC boosts IT investment ahead of UK government's new digital modernisation plans


The Department of Health and Social Care (DHSC) has significantly ramped up its investment in digital devices over the past three years, spending more than £3.6 million on laptops, mobile phones, and iPads to support remote working initiatives.

This increase in funding coincides with the government's broader commitment to modernise the NHS and social care sectors, announced earlier this year during the Spending Review 2025. The UK government has pledged up to £10 billion by 2028-2029 to strengthen the healthcare workforce and accelerate digital transformation across health and social services.

Data obtained through a Freedom of Information (FOI) request and analysed by the Parliament think tank reveals that the DHSC's total expenditure on electronic devices over the recent period amounted to £3.6 million. Of this, £3.1 million was spent on laptops, demonstrating a primary focus on portable computing devices. Mobile phones accounted for approximately £380,468, while iPads made up around £91,115 of the total expenditure.

The data shows a notable rise in DHSC's annual spending on staff technology from 2022 to 2025. In 2022-2023, the department spent approximately £530,443, which increased significantly to a peak of nearly £2.85 million in 2023-2024.

This surge was primarily driven by a substantial increase in laptop purchases, which jumped from £500,414.08 to around £2.63 million year-on-year, before reducing to roughly £248,029 in 2024-2025. This pattern indicates a focused effort to modernise the digital tools available to health and social care staff, supporting the government's wider digital health strategy. ■



ELEVATE
Future Faster
nvent
SCHLEIFENBAUER

PDU RePower: Trade in for Tomorrow

Ready to upgrade your power infrastructure and make a positive impact?

Get up to £35 off each PDU when you trade in.

Get started today. Reach out to the Elevate team:
elevate@excel-networking.com | 0121 326 2471


Terms and conditions apply.
Programme runs until 31 Dec 2025.


POLE POSITION: AWS


Data Centres in the Fast Lane

Join us for an electrifying afternoon where innovation meets acceleration. Whether you join Elevate for the ideas and discussions or the immersive F1 racing simulators, this will not be your average event.

9th October | St Paul's, London | Half-Day Event | Starting 12:00pm







Powering Resilience for 16 Years

Since 2009, Critical Power Supplies (CPS) has provided reliable backup power solutions, helping organisations across the UK maintain uptime and continuity. Our focus on resilience, reliability, and customer service allows us to deliver tailored UPS, power distribution, and critical service support to industry standards.

Over the years, CPS has evolved with the industry, meeting the growing demands of digital infrastructure, data centers, and critical applications. Today, CPS benefits from strong partnerships with leading OEMs such as APC, Riello, Eaton, and CyberPower. These alliances give our customers access to best-in-class technology backed by manufacturer-certified expertise.

At CPS, customers are more than clients; they are long-term partners. We invest time to understand each organisation's challenges and deliver tailored backup power strategies. Our white-glove approach ensures all solutions, from design to maintenance, are crafted for maximum business continuity "when it matters most."

Our skilled engineers and response teams form a nationwide support network. With proactive maintenance, fast emergency assistance, and comprehensive care, CPS ensures peace of mind for organisations that cannot afford downtime.

At the heart of CPS's success are its people: experienced engineers and support staff with decades of collective knowledge. Their expertise ensures our maintenance, emergency support, and system care meet the highest standards. With our dedicated Service Team and advanced field service tools, CPS delivers faster responses and greater customer visibility. Looking ahead, we are building long-term resilience, supporting the shift to smarter, connected infrastructure, and ensuring CPS remains the benchmark for reliable backup power and peace of mind for organisations that cannot afford downtime.

CPS solutions are trusted across many sectors, including:

- Data centres & IT infrastructure
- Healthcare & emergency services
- Education & public sector
- Transport & logistics
- Commercial and industrial operations

For 16 years, CPS has powered resilience. We continue to invest in people, partnerships, and technology to secure the future of critical infrastructure.

www.criticalpowersupplies.co.uk
0800 978 8988
sales@criticalpowersupplies.co.uk



UK private sector heavily dependent on US technology

Recent research reveals that the UK private sector relies extensively on US technology to operate vital systems, with 88% of publicly listed companies depending on American services.

This heavy reliance is reflected across several European countries, with Ireland showing a 93% dependence, France at 66%, Portugal at 72%, and Spain at 74%, based on a study by Proton analysing email service providers as a proxy for broader technological dependence.

Email infrastructure, a critical component for communication, data storage, and employee identification, represents a significant strategic asset. The study indicates that in key sectors — such as banking and telecommunications — up to 95% of publicly listed companies depend on US-based technologies. Utilities, transportation, and energy sectors also display high reliance, with dependency rates above 80%. Even the UK's technology industry, valued at US\$1.1 trillion, shows substantial US dependence: approximately 94% of software and services firms and 82% of hardware manufacturers listed domestically utilise US platforms.

This pervasive dependency raises long-term concerns about Europe's digital sovereignty. Analysts warn that reliance on foreign technology providers limits control over critical data, hampers domestic innovation, and exposes economies to vulnerabilities during geopolitical crises. Proton emphasises that this over-reliance creates a "dangerously vulnerable" posture, risking significant disruptions to business continuity and national security if foreign providers face technical failures or geopolitical conflicts.

The report laments decades of complacency, where Europe's preference for overseas solutions over local development has compromised its strategic independence. Such dependence restricts the continent's ability to safeguard sensitive data and foster home-grown innovation, potentially rendering Europe increasingly vulnerable and economically constrained. The authors call for urgent action, advocating a "Europe First" approach to develop local digital infrastructure, support national talent, and reduce external vulnerabilities.

Proton urges policymakers and businesses to prioritise investments in domestic technologies and open-source solutions, which could bolster privacy, ensure service continuity, and align with European values and regulations. While email infrastructure is highlighted as a key vulnerability, the report signals broader concerns about technological dependence across various domains. It emphasises the need for Europe to take decisive measures to reclaim control over its digital future, encouraging the development of resilient, locally rooted ecosystems that support sovereignty, security, and economic growth. ■

Cornwall faces risk of mobile blackspots amid rent dispute

Cornwall could be at risk of losing vital mobile coverage as landowners warn they may refuse to host phone masts due to significant rent reductions. Local landowner groups and residents have expressed concern that recent government plans to extend the existing rules could further jeopardize connectivity across the region.

Changes introduced in 2017 to the electronic communications code granted mobile operators sweeping powers to slash payments to landowners — many of whom are farmers, small business owners, local authorities, and NHS trusts — resulting in rent cuts of up to 90%. These measures were intended to accelerate the rollout of mobile infrastructure but instead led to over 1,000 legal disputes, a stark increase from just 33 cases in the previous three decades.

This legal and regulatory turmoil has contributed to a slowdown in the deployment of new mobile masts, contradicting the policy's original aim. The UK currently ranks near the bottom among European countries for 5G

coverage, with only 45% of the population covered, compared to more than 80% in nations like Denmark and Finland. The prospect of further regulatory changes has raised fears that rural and underserved areas like Cornwall could face even greater connectivity challenges if landowners choose to withdraw their support for new infrastructure. ■



Cyber skills shortage drives UK organisations into risky security practices

A recent report highlights a growing crisis across the EMEA region, where many organisations are resorting to risky cybersecurity practices due to a widespread shortage of skilled professionals.

Insight's research indicates that 64% of organisations in Europe, the Middle East, and Africa are relying on temporary fixes and workarounds to cope with mounting cybersecurity demands. The situation is particularly severe in the UK, where 67% of organisations report a cybersecurity skills shortage, with more than half describing the impact as "severe" or "significant." The deficit is most acute at senior levels, with many respondents citing a lack of expertise in strategic areas such as governance, planning, and risk assessment.

Across the broader region, only 24% of IT decision-makers believe their organisations possess sufficient in-house cybersecurity skills to keep pace with evolving threats. Consequently, over half of the surveyed businesses report delays in critical projects or technology initiatives,

and an equal proportion struggle to meet compliance requirements due to a scarcity of cybersecurity expertise.

The study identifies the high cost of hiring and training as the primary obstacle, with 68% of IT leaders citing this as a key barrier. Additionally, 65% point to the limited availability of qualified candidates in the market. The skills shortage extends beyond technical roles to operational, leadership, and compliance positions, undermining both daily resilience and long-term strategic planning.

The UK figures are particularly stark, with more than half of organisations experiencing "severe" or "significant" impacts from the skills shortage. These include delays in key projects and challenges in compliance, mirroring the overall EMEA trend. The report concludes that until organisations can address both financial constraints and talent shortages, many will continue to rely on temporary security measures that increase their vulnerability to cyber threats. ■

Word on the web...

UK faces a new era of wireless... again

Scott Baxter, Network Systems Consultant, Velaspan

To read this and other opinions from industry luminaries,

visit www.networkingplus.co.uk





Beyond data placement: rethinking data infrastructure at the source

Mark Klarzynski, Co-Founder & Chief Strategy Officer, PEAK:AI0

For decades, data architecture has been built around a simple assumption: storage is where data lives, and compute is where the work gets done. But as AI scales, this traditional separation is becoming a major obstacle. Networks are overloaded, power consumption is surging, and latency often leads to missed opportunities.

To move forward, we need more than small improvements. Smarter caching layer or better tiering may buy time, but they're not sustainable solutions for the long run. What's required is a fundamental shift in how we think about data and computation, and not just where data is stored, but where computation actually happens.

Let's pause on that. "Stop bringing the data to the job. Start bringing the job to the data."

Imagine a common enterprise scenario: a simple SQL search across a multi-petabyte dataset. Traditionally, storage sends the data across the network to a compute server, which caches it, then processes the query. However, today's datasets are too large, and the costs of bandwidth, time, and energy are too high.

As businesses today need to make decisions in real time, any friction in the data pipeline can create issues and pose risks. What if we flipped the model and the storage system didn't just serve data, but actually processed it?

This isn't a novelty, but a strategic rethinking. By enabling computation directly within the storage platform, organisations can significantly reduce latency, network usage, and infrastructure costs, all while meeting the demands of AI at scale.

Compute at the edge of storage

This concept has implications far beyond SQL. Consider AI inference pipelines, real-time analytics, or machine learning workloads where response time matters. Many of these tasks are highly parallel and read-intensive, making them ideal candidates to run closer to the data.

Allowing architectures to place containerised inference models directly on the storage node enables operations such as vector similarity searches, metadata filters, or preprocessing steps to occur directly where the data resides, before a single byte is transmitted over the network. This shift not only improves performance but also saves on cost by reducing data fees, network congestion, and energy usage.

When implemented properly, this doesn't just reduce latency, but it reshapes what's possible.

Intelligence isn't just in the workload. It's in the movement.

While this rethink of job placement is transformative, it's only half of the equation. For this model to reach its full potential, data must already be where it needs to be, when it's needed.

Modern architectures are now evolving to enable multi-tiered, intelligent data management that goes far beyond traditional tiering. This means seamlessly integrating diverse storage types, such as high-performance NVMe, QLC flash, archive-class media and even cloud storage, into a unified, transparent system.

However, it's not about just unifying layers. Instead of relying solely on static policies or predefined rules, advanced systems now use AI-driven engines to monitor real-time usage, access frequency, and workload behaviour. Data is then automatically moved or replicated based on performance needs, relevance, or projected demand, without introducing latency or disrupting users.

As a result, the right data is placed in the right location at the right time, often before it's even requested.

From edge to exascale

This intelligent, active approach to data isn't limited to large-scale cloud environments. In fact, it's often most valuable in smaller power or space-constrained settings, where power, space, and bandwidth are limited, and latency can't be masked by overprovisioning.

Whether at the edge, in healthcare deployments, or within large-scale research

institutions, the principles remain the same: storage must be efficient, autonomous, and aware of the data it serves.

By combining highly efficient storage infrastructure with intelligent, workload-aware data management, organisations can extend the benefits of AI-driven architectures from edge devices to exascale systems.

Time to rethink storage's role in AI

As AI workloads grow, the underlying infrastructure philosophy must evolve too. Simply adding more GPUs or scaling flash

storage is no longer a sustainable strategy, either financially or environmentally.

The real opportunity lies in a systemic rethink: building infrastructure that is not just faster, but smarter, making storage an active part of the AI pipeline, rather than a bottleneck to work around.

By combining intelligent data movement, in-place job execution, and dynamic tiering into one cohesive system, infrastructure can become more autonomous, efficient, and responsive to the growing demands of workloads.

This isn't just about keeping up, but about reimagining what infrastructure can be with AI. ■

APC

Uninterruptible Power...

REDEFINED

The future of uninterruptible power.

Find out how one small change can be the big solution to your IT challenges. Watch the video.

Smaller. Lighter. More powerful.

Meet the innovative APC Smart-UPS™ Ultra that's driving the future of uninterruptible power

The most sustainable UPS of its kind, the Smart-UPS Ultra is now available with improved battery life. It is capable of remote monitoring and supports extended runtime options.

www.apc.com

Life Is On | **Schneider** Electric

How third-party breaches put retail networks at risk



Kevin Curran, IEEE senior member and professor of cybersecurity at Ulster University

In the space of just a few weeks, many high street and online retailers were impacted by serious cyber incidents that disrupted their business-critical services earlier this year. Ecommerce platforms were knocked offline and physical payments systems were temporarily unavailable. These incidents were a harsh reminder of how vulnerable retailers are when their networks are so closely tied to third-party suppliers and service providers.

Why attackers target the supply chain

The retail sector's reliance on external vendors for services like payment processing, logistics, customer analytics and marketing has created new entry points for attackers. These partners are often granted access to sensitive systems or customer data but may not maintain the same level of cybersecurity maturity as the retailers themselves, leaving a weak link in the supply chain. Smaller retailers are especially exposed, as limited cybersecurity resources can make them easier targets for attack.

Regardless of size, once third-party vendors are given access, it takes just one compromise to put an entire network at risk. The 2013 Target incident is still one of the most cited examples of third-party risk, where attackers used stolen credentials from an external HVAC vendor to gain entry to the network, exposing more than 41 million credit card records.

Today, cybercriminals are still exploiting these gaps, targeting weak vendor access points, remote connections and cloud integrations as convenient gateways into larger and better-protected organisations. The ongoing shift towards cloud-based services and SaaS platforms has also increased the attack surface.

On top of supply chain weaknesses, the data retailers hold – from payment details to loyalty scheme information to customer records – makes them attractive, lucrative targets. Regulators add to the pressure by holding the primary business accountable for breaches, even if they originate with a partner. Under GDPR, for instance, brands remain responsible, which means retailers will need to get a handle on third-party risk or face significant reputational and financial damage.

Defending retail networks

Retailers need a layered approach to security, covering people, processes and technology. This starts with re-evaluating the vendor selection process to make sure all partners follow recognised standards like ISO 27001, SOC 2 or PCI DSS. Security requirements and breach reporting obligations should be written clearly in contracts and SLAs from the outset.

Once relationships are in place, tighter access controls are needed. A Zero Trust model ensures that third parties only have access to the data and systems they genuinely need. Multi-factor authentication (MFA) should also be enforced across all third-party connections. The Snowflake breach in 2024, which took advantage of single-factor

authentication, is a good example of how dangerous weak access protocols can be.

Network segmentation is an important safeguard, adding an extra layer of protection by isolating critical systems such as PoS terminals and customer databases. By keeping these areas separate, any compromise can be contained before it spreads. In fact, many of the most damaging breaches in recent years could have been reduced had this been in place.

However, segmentation alone is not enough. Modern retailers operate in an environment where threats advance quickly and supply chains are constantly shifting, which makes continuous monitoring vital. Tools that can detect unusual behaviour across third-party connections provide early warning of suspicious activity and give security teams the chance to intervene before small issues escalate into major incidents. Additionally, cyber insurance policies should be reviewed carefully to ensure they cover breaches involving third-party vendors, as not all of them do.

Lastly, people within the organisation play an important role too. Staff need to be trained to recognise warning signs and incident response plans should be tested regularly with vendor-related scenarios included. No defence is flawless, but the ability to act quickly and decisively can make all the difference.

Looking ahead

In time, third-party breaches will become more frequent and more sophisticated. Attackers are already using AI to spot vulnerabilities faster, scan for weaknesses at scale and automate parts of an attack. This makes it easier to exploit even the smallest gaps in a retailer's digital supply chain.

Regulators may also tighten enforcement of laws such as GDPR, with heavier fines for organisations that fall short on third-party risk management. For retailers, that means treating vendor security as part of their own and rethinking how they work with partners, with greater emphasis on transparency, ongoing risk assessments and recognised certifications. At the same time, demand for automated third-party risk management platforms is expected to grow, giving retailers real-time visibility across their supply chains.

Some may adopt secure-by-design practices to limit reliance on suppliers for sensitive data, while others could bring security into development cycles earlier through DevSecOps and continuous penetration testing.

Attackers are very opportunistic and will always hunt for weaknesses among third-party vendors, cloud platforms and other outsourced providers. Rather than backing away from these important relationships, retailers should focus on raising the standard of security across every connection.

With greater accountability, stronger governance and tighter control across the ecosystem, this shift should be seen as a positive step for the sector and its customers. ■

Independant UK Datacentres & Server Hosting

Who we support:

Clients ranging from **national & multinational companies** to **schools** and **small businesses.**

0800 084 3521
www.veloxserv.co.uk



MobileMark

antenna solutions

STAY CONNECTED

with Advanced 5G
Antenna Solutions for
Autonomous Vehicles,
Public Transportation,
Precision Agriculture,
Medical IoT, Robotics,
and More!

www.MobileMark.com

Contact Us Now:
+44 1543 459555
enquiries@MobileMarkEurope.co.uk



Buy, rent, stream?

The Netflix-ification of enterprise IT

In today's UK enterprise landscape, the decision to rent, buy, or outsource IT equipment is about more than budgets — it's about agility, security, and futureproofing. We explore how businesses can align their IT strategy with long-term goals...

When it comes to IT equipment, UK businesses face a deceptively simple question: should you buy it, rent it, or hand the whole thing over to a managed provider?

On the surface, it feels like a basic budgeting issue. Do you want the shiny new laptop paid off in one go, or the manageable monthly bill? But scratch deeper and you'll find that the choice touches everything from cash flow and compliance to how efficiently your staff work on a Monday morning.

CAPEX vs. OPEX: the age-old tug of war

Let's start with money, because that's where most boardroom conversations start.

If you buy equipment, you're in CAPEX territory: a big upfront outlay, depreciated over time, with all the joys and

headaches of ownership.

"Enterprises evaluating whether to purchase, rent, or build IT equipment often begin by comparing CAPEX, which involves a larger upfront investment, with potential ongoing OPEX to cover licenses and maintenance associated with the hardware vendor," says Vince Jouan, VIP EMEA at Wifirst.

Meanwhile, if you rent or go down the 'as-a-service' route, you shift spend to OPEX, paying monthly and keeping your cash flow free for other priorities.

"Adopting an 'as-a-service' or rental model maximises the long-term value of IT investments by ensuring robust and reliable infrastructure while allowing internal resources to focus on services that directly support business objectives. Costs are spread over time, freeing available cash for other strategic operations," says Jouan.

Mark Darrah, Cloud Practice Lead at Arc, has seen a split in the market between

the SMEs and large corporations when it comes to their equipment ideals.

"I can see the trend is moving towards rented hardware solutions, allowing SMEs to manage costs on the monthly basis rather than large capital purchases. Similar to SaaS-based solutions, there is an argument to say hardware could also go that route; renting allows the foresight of easier asset management and replacement, which is often more difficult to manage in smaller organisations," observes Darrah. "Larger corporates, I believe, will continue with capital purchases as they have the resource to manage devices and refresh with enterprise tools. In terms of cost implications for SMEs, this is more relevant to keeping staff working efficiently with refreshed hardware on a regular basis which renting offers. Also, the security aspect of having outdated systems could lead to compromise costing SMEs tens of thousands."

It makes sense. Smaller companies often don't have the luxury of tying up capital in equipment that will be obsolete in three years. Renting is like Netflix for your IT kit: you don't own it, but you get the latest version when you need it, and you don't worry about what happens when it's out of date.

"We are often asked about 'rent or buy hardware' but the first question is where should I place the organisation's workloads, such as core ERP applications, real time manufacturing/processing apps, to standard finance systems or



Mark Darrah, Arc

end-user applications?” asks Andy Harris, CCO, ITPS. “Ultimately, this is not simply a financial calculation about leasing models. It is a strategic choice between the control and predictability of CAPEX-driven hardware and the agility and scalability of OPEX-driven cloud services.”

In other words, if you're only comparing costs, you're missing half the story.

Performance, latency, and the Monday morning test

Numbers on spreadsheets are one thing. But how does each model feel on a Monday morning when your finance team logs in, or when your design engineers start throwing huge CAD files around?

Buying your own kit means you control performance. You can handpick specs, tweak configurations, and squeeze every drop of power for your workloads. But hardware ages fast. That top-of-the-line server you bought three years ago may now be the digital equivalent of running a Ferrari with 200,000 miles on the clock.

“Purchasing hardware provides direct control over configurations, enabling IT teams to optimise for specific workloads,” asserts Jouan. “However, aging equipment, limited refresh cycles, and the challenge of maintaining uniform standards across hundreds of sites can impact both reliability and latency over time.”

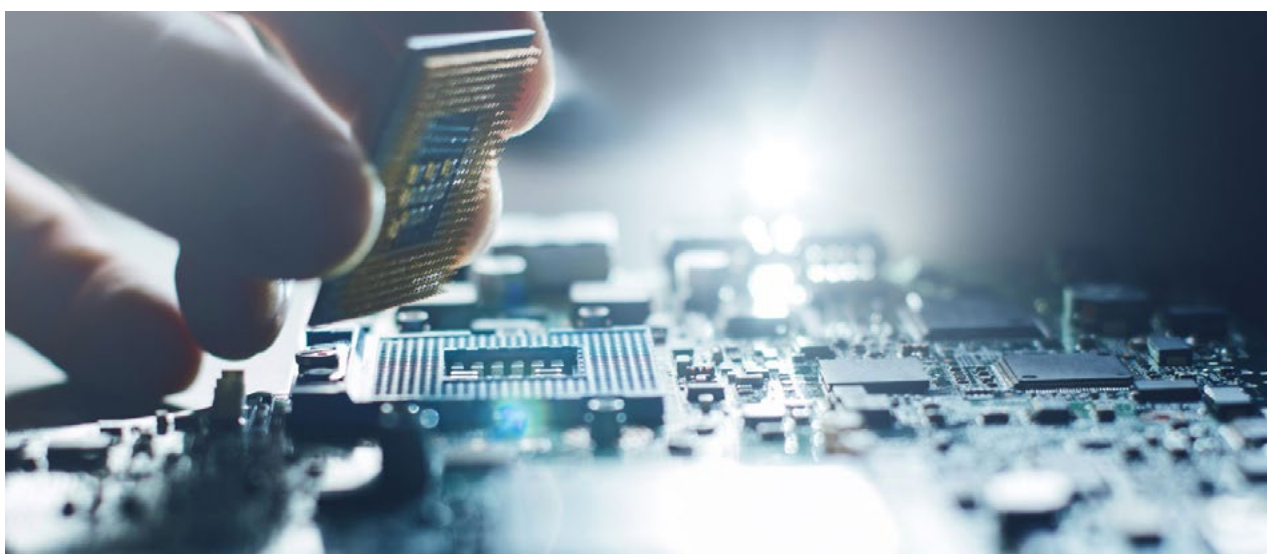
“Older computers left past a period of 3-5 years has an impact on the user's performance if they are reliant upon the local compute,” adds Darrah.

Custom-built infrastructure sounds good in theory — you get exactly what you need. But Jouan warns that in practice it's “difficult to achieve consistent reliability at scale.” Without industrialised processes and armies of engineers, bespoke setups can become fragile.

Managed services and rental options, however, come with performance guarantees.

“Managed services provide performance and reliability guarantees through Service Level Agreements (SLAs),” shares Jouan. “Providers can leverage scale to maintain uniform configurations, perform proactive monitoring, and resolve issues quickly. This approach also enables optimisation for latency-sensitive applications and continuous equipment refresh, which is critical for digital services that rely on high-speed, reliable connectivity.”

Darrah also points to the growing role of VDI (virtual desktop infrastructure): “monthly rental or leasing for SMEs means they can bring higher performance machines without huge capital outlay —



for example, CAD-based machines. Latency only really becomes an issue with VDI-based environments whereby the networking between the user and the cloud-based compute are poor.”

So, the Monday morning test? Bought hardware provides control but risks age and obsolescence. Rented and managed solutions mean less tinkering, more guarantees — and fewer coffee-spilling crises when things grind to a halt.

Integration: the devil in the details

Of course, performance is only part of the story. There's also the question of how all this stuff actually fits together.

Buying gives you customisation freedom — you can pick and mix hardware to suit your workloads. But as anyone who's ever tried to connect a ‘standardised’ system with a decade-old ERP platform knows, integration isn't always straightforward. Testing, patching, maintaining — it's a never-ending process.

Darrah highlights that while purchasing allows for stronger customisation in terms of compute, which is certainly more restricted in a rental market, “there may only be a few options open to rented machines — for example, standard build, CAD build, video editing base. Some applications require higher throughput from a CPU or storage perspective. Special requirements such as custom OS or deployment in rental can also be an issue and could be limited for mass deployment models.”

“Purchasing hardware typically involves standardised, off-the-shelf components,” confirms Jouan. “While this simplifies basic interoperability, integrating them with legacy systems or diverse applications (such as ERP, digital signage, IoT devices, and sensors) requires significant internal effort, including configuration, testing, and ongoing maintenance. Maintaining up-to-date infrastructure also demands dedicated R&D resources to keep pace with evolving standards and integrations.”

Indeed, one thing often overlooked in the rent vs. buy debate is the people side. Hardware doesn't maintain itself. Buying means in-house IT teams are constantly juggling refresh cycles, firmware updates, and troubleshooting across multiple sites.

“With a purchased hardware scenario, you will be constantly working with maintaining the physical kit in various different avenues across multiple locations. This can make upgrades, policy, refreshing kit expensive and difficult to manage,” opines Darrah. “With rented VDI, there is far more automation and administration using

that single pane of glass is easier and does not require techs as many complicated tasks are automated.”

“WiFi deployment in increasingly complex environments is a highly specialised field,” says Jouan. “Organisations benefit from partnering with operators fully focused on network design and R&D, capable of leveraging extensive experience and structured processes to operate these services efficiently. Specialist operators develop, deploy, and manage networks at scale every day, whereas internal teams without dedicated radio and network expertise face steep learning curves and operational risks.”

In short, the technical expertise required to maintain, troubleshoot, and upgrade large-scale WiFi infrastructure is significant. Increasingly, outsourcing or utilising the as-a-service model becomes more attractive to enterprises large and small.

“The ‘as-a-service’ model provides a more robust solution. For an AAS operator, success depends on delivering a fully functional service from day one. Any errors affecting clients during a contract (typically five years) are the provider's responsibility, creating a strong incentive to deploy future-proof infrastructure that ensures seamless integration with a wide range of devices and applications,” explains Jouan. “Additionally, AAS providers, given their scale and volume, carry significant influence with hardware manufacturers, enabling them to stay aligned with market trends and customer requirements.”

Scalability: From Start-Up to Scale-Up

Here's a thought experiment: imagine your business doubles in size overnight. Could your IT keep up?

Scalability is where ownership often shows its limits. Bought hardware ties the enterprise to a point in time. If you suddenly need more compute power or storage, you're looking at weeks of procurement and installation.

Indeed, “in the purchase scenario, you are fixed to a point in time in terms of the hardware you have invested in and the same is true for a period with rental,” says Darrah. “If we are looking at VDI, then it is extremely scalable with the ability to switch out a machine and the compute within a few minutes. VDI allows for many different compute, storage and graphics requirements with flexible switch out plans.”

“Scalability is critical for enterprises anticipating growth in data throughput, storage,

and network bandwidth,” says Jouan. “Although theoretically scalable, deploying and operating a large-scale, versatile network internally requires substantial tooling, processes, and development resources. This is particularly challenging because infrastructure is often treated as a cost centre rather than a business differentiator. As a result, network expansion can be slow, resource-intensive, and difficult to maintain consistently across multiple sites.”

So... rent, buy, or build?

The ultimate answer to the ‘rent, buy or build’ question is that it depends.

SMEs often benefit most from renting and VDI. Predictable costs, easy scalability, and less compliance burden keep them lean and competitive. Large corporates, on the other hand, still find ownership valuable, especially when economies of scale kick in. With big IT teams and structured processes, they can manage refresh cycles without breaking sweat. Meanwhile, for performance-critical industries like high-frequency trading or real-time manufacturing, on-premises kit is required to guarantee low latency. And for fast-growing companies, agility and scale will struggle without OPEX-driven models.

According to Harris, “the right path depends less on ownership models and more on the operational priorities of the enterprise in the context of a right-sized business case.”

IT strategy is no longer about hardware versus cloud, or CAPEX versus OPEX. It's about what kind of organisation you want to be: one that values control, or one that prizes agility. ■



Vince Jouan, Wifirst



Andy Harris, ITPS



The compliance time bomb: how on-prem storage and legacy backups are putting e-discovery at risk

James Griffin, CEO at CyberSentriq

Data is growing faster than most businesses can manage, and cloud productivity tools alone can't keep up. When security, compliance, and retrieval are at stake, MSPs need more than great storage - they need control.

UK IT security regulators don't care how your data is stored - just that it has protections in place and you can find it, fast. However, for MSPs and IT teams still fighting the good fight with on-premise storage and legacy backup systems, e-discovery is a ticking compliance time bomb.

Alongside this, UK data regulators are cracking down and handing out harsher penalties for data malpractices. To stay compliant, businesses need to be on top of all of their data assets, making them secure and reachable, on demand, at all times.

To meet modern compliance demands, MSPs need a single platform that can search, secure and scale without manual patchwork or blind spots. A unified e-discovery platform doesn't just protect data, it makes ditching fragile, outdated storage systems simple and secure.

Compliance obligations

Staying compliant at scale is a major challenge for growing companies, especially as data volume, regulations, and complexity increase. When managing data across the IT estate, businesses need to be fully prepared well in advance of auditing and regulatory enquiries.

In the UK, businesses must be able to identify where all the electronic information they oversee comes from. Disclosure and inspection of documents is mandated under Part 31 of the Civil Procedure Rules, and regulations are being revisited frequently in Parliament. Full data compliance encompasses email, databases and other internal files - all of which are ever-changing.

Whether it is a customer exercising their fundamental right to personal data or legal officials enquiring about certain assets, the right information needs to be immediately accessible. However, for businesses with disparate and siloed on-premise storage, search difficulties occur, and the systems involved are incapable of tracking changes in content or location.

If such information is lost, financial damage in the form of fines, as well as reputational damage in the eyes of the customer involved, are risks that no business can afford.

Cloud-based e-discovery

e-discovery automates the vital process of locating and retrieving data, accelerating the demonstration of due diligence and decreasing the strain on staff. This capability remains flexible in line with evolving legislation, helping firms to stay proactive with their data management. But without a central location for data management that is accessible from any company device, legally enforced search and retrieval is bound to remain complex and costly.

Full control over data, identities and communications - along with the high costs that can otherwise come with e-discovery - can be ensured by centralising this capability in the cloud. Cloud infrastructure allows organisations to scale costs up and down, and only pay for the resources they need.

Specific assets can be instantly located across multiple storage environments, ensuring legal requests are met without



delay. This is paramount in a business world where every piece of digital information almost certainly resides in more than one location.

Optimising backup and security

The ability to properly back up and secure all data at the organisation's disposal, across cloud and on-prem environments, is also a key element of compliance that plays into any strong e-discovery tool. As data breaches must be reported to the Information Commissioner's Office (ICO), it makes sense to optimise authentication and security of sensitive information before regulatory queries arise.

For best results, the cloud-based e-discovery tool you implement should adhere to ISO 27001, ISO 9001, ISO 22301, SOC 2 Type 1 & 2, and (for healthcare-associated businesses) HIPAA standards. The cloud platform acquired needs to be fully tailored to the specific regulations that oversee the industry in which the MSP, enterprise or IT team operates.

Additionally, cloud-based e-discovery should be capable of keeping all data immutably backed up and scannable before recovery, to help avoid any corruption as a result of rising malware threats.

Tackling data growth with ease

The old, convoluted way of manually checking on data in each business department and reactively putting measures in place is prone to delays and no longer cuts it in a business world that demands fast-paced action. Moving e-discovery to the cloud would go a long way in facing evolving regulations and legal queries head-on.

Cloud-based e-discovery inherently scales to encompass masses of data coming into the company network as a result of internal and external communications, as well as administrative and project management. It doesn't end with speeding up and streamlining search and retrieval; cloud infrastructure centralises and boosts data security, with access and privileges being customisable in line with the specific needs of the business.

By investing in e-discovery tools that work seamlessly across cloud environments,

organisations can amply prepare for, and quickly satisfy, any customer or regulator challenge that comes their way.

But more than just a compliance safeguard, this investment becomes a strategic enabler, transforming how organisations manage risk, respond to incidents, and even make decisions.

Modern e-discovery platforms that integrate across cloud apps (like Microsoft

365, Google Workspace, Slack, and Zoom) not only ensure rapid access to data but also provide intelligence and context, surfacing patterns and behaviours that would otherwise stay buried in data sprawl.

Regulations are tightening. Customers expect control, and the cost of non-compliance is only going up. It's time for MSPs to stop firefighting and start building a foundation for confident, compliant growth. ■

HARNESS THE POWER OF ZOOK...

Remotely Monitor Basic & Metered PDUs

USE POWERZOOK TO IDENTIFY

- PDU power usage
- Power failure
- Equipment failure
- Near-overload conditions
- Unusual power usage patterns
- Cable/wiring faults



WHY POWERZOOK?

- No downtime installation
- Clamps around 3-core cables
- No cable modification needed
- PoE
- SNMP
- No additional point-of-failure
- Easy swap-out if needed

Jacarta

SENSORS FOR THE DATA CENTRE & BEYOND™
pz@jacarta.com | www.jacarta.com
+44 (0)1672 511 125



Strategies for network optimisation

As UK organisations face soaring digital demands, network optimisation has shifted from a technical challenge to a business imperative. This feature explores how scalable design, intelligent tools, and airtight security can future-proof IT infrastructures...

Optimising IT networks in the UK isn't just about speed — it's about building infrastructures that can adapt, self-heal, and scale in line with ever-growing demands.

"Comprehensive network planning starts with understanding how people and devices interact with the environment," says Gerard Donohue, Chief Technology Officer at Telent. "By analysing data from connected systems like sensors, cameras, and endpoints, it's possible to predict where bottlenecks are likely to emerge and plan accordingly."

Hamzah Malik, Solutions Consultant, CACI, agrees, stressing that modular, hierarchical design is key to scalability: "comprehensive planning and scalable design are the foundation of a future-proof network. Modular architectures allow organisations to scale capacity without re-architecting the entire infrastructure. With tools like network modelling, capacity planning, and SDN, businesses can anticipate demand and flex bandwidth as needed."

Together, these strategies mean organisations can scale intelligently — avoiding costly redesigns and ensuring networks grow as fast as their businesses.

Why cutting corners on equipment costs more

Cheap hardware may seem like a bargain, but it can cripple performance and security in the long run. Investing wisely is key.

"Enterprise-grade equipment from trusted vendors like Cisco, Juniper, and Fortinet undergoes rigorous testing, offers advanced telemetry, and benefits from ongoing software support. This investment translates to greater stability, better visibility, and improved automation capabilities, which ultimately lowers operational costs over time. Cutting corners often leads to downtime, vulnerabilities, and scaling challenges," asserts Malik.

Indeed, investing in high-quality networking equipment from reputable vendors ensures the foundation of a reliable, secure, and high-performance infrastructure. Systems with built-in intelligence enable automated diagnostics, real-time monitoring, and predictive analytics, reducing downtime, simplifying maintenance, and allowing faster resolution of issues resulting in an improved user experience.

"For example, Oxford University deployed

a Juniper Mist Wi-Fi network that uses AI to deliver continuous diagnostics and configuration recommendations across all campus access points," highlights Donohue. "This approach ensures consistent performance, strengthens security, and supports growing demands without constant human oversight."

In short, high-quality kit isn't just more reliable — it comes with the intelligence and vendor support needed to keep pace with evolving demands.

Getting smart about traffic

When every device is talking at once, prioritisation becomes non-negotiable.

"Managing bandwidth effectively starts with understanding how traffic moves through a network and applying intelligent controls to keep critical services running smoothly. With connected devices generating constant data, AI-driven analytics can detect congestion, identify performance issues, and automatically allocate resources where they're needed most," explains Donohue.

Quality of Service (QoS) techniques play a key role here by prioritising essential applications such as mission-critical systems or real-time collaboration platforms over non-critical traffic.

"By combining traffic analysis with automated QoS policies, organisations can ensure that their most important services receive guaranteed bandwidth and maintain performance even during peak demand," adds Donohue.

Malik notes that QoS techniques ensure mission-critical apps don't get bogged down: "traffic analysis provides deep insights into how bandwidth is consumed and where congestion points arise, enabling informed decisions about optimisation. QoS then ensures mission-critical applications — such as VoIP, collaboration tools, and business systems — are prioritised over less time-sensitive traffic."

This not only improves user experience but also maximises the value of existing infrastructure by aligning bandwidth allocation with business priorities.

"Advanced network analytics tools and AI-driven telemetry can now automate much of this process, making it easier to dynamically adapt to changing traffic patterns," notes Malik.

Further, uptime doesn't happen by accident; it's engineered.

"Uptime is an architecture choice. Redundancy and failover aren't optional — they're essential for any organisation that depends on uptime," claims Malik. "Protocols like STP, VRRP, and advanced routing convergence mechanisms ensure high availability, preventing single points of failure. This is particularly crucial as more workloads move to hybrid and multi-cloud environments, where network downtime directly impacts customer experience and revenue. Designing redundancy into both the hardware and software layers is the most cost-effective insurance policy for modern enterprises."

"While traditional network protocols like Spanning Tree Protocol (STP) are designed to prevent loops and ensure traffic reroutes in the event of a switch failure, modern smart infrastructure builds on these principles by adding layers of intelligence and automation," adds Donohue.

Security: the invisible backbone of optimisation

If networks are living systems, then monitoring is the pulse check.

Malik explains that "what works today may not meet tomorrow's demands. Continuous monitoring provides real-time visibility into health, utilisation, and security, enabling teams to act proactively rather than reactively. Regular assessments ensure design, performance, and security stay aligned with business growth, regulatory requirements, and evolving threats. Optimisation isn't a one-off project — it's an ongoing discipline."

Donohue echoes this with real-world examples: "in high-footfall public environments like transport hubs, 24/7 remote monitoring of access points and switches ensures consistent availability and quick response to issues. Scheduled maintenance combined with rapid fault resolution helps maintain quality of service. Similarly, in education environments, platforms like Juniper Mist provide AI-driven diagnostics and configuration updates to proactively manage performance. These examples highlight how continuous assessment, supported by intelligent tools, keeps networks reliable, adaptable, and ready for whatever comes next."

Every IT team knows that, as networks

become faster and more interconnected, their attack surface grows, making robust security measures more critical

"Next-generation firewalls, intrusion detection and prevention systems (IDS/IPS), and secure segmentation are key pillars of a zero-trust architecture, ensuring that performance improvements never come at the cost of security," warns Malik. "These should be complemented by endpoint detection and response (EDR), anomaly-based analytics, and automated threat response to stop ransomware, phishing, and insider threats in their tracks. In addition, antivirus and anti-malware tools remain essential layers of defence to block and isolate threats before they spread."

Donohue agrees that firewalls and intrusion detection systems are foundational to defending against modern cyber threats, providing the first line of defence, with firewalls controlling access and blocking malicious traffic, and intrusion detection systems monitoring activity across the network to identify and alert on suspicious behaviour.

"In sectors like education, where cybercrime incidents have surged and the industry now ranks among the top five global targets, these protections are more important than ever," shares Donohue. "AI-enhanced security adds a further layer by offering real-time visibility into who is accessing the network, from where, and under what conditions, giving IT teams the insight needed to detect, assess, and respond to threats before they escalate."

Technology alone, however, is not enough: comprehensive user training is vital to build a human firewall, empowering staff to spot phishing emails, social engineering tactics, and other malicious activity.

"A truly optimised network is not only fast and scalable but inherently resilient, with both technical safeguards and well-informed users acting as front-line defenders," comments Malik.

The takeaway? An optimised network isn't just fast — it's resilient against evolving threats.

The bottom line

From scalable design and intelligent traffic management to security-first architectures and continuous monitoring, the principles of network optimisation are clear: plan for growth, invest wisely, automate wherever possible, and never treat optimisation as 'finished.' ■



The frontline isn't forgiving – neither should your communications be

Alasdair Ambroziak, Head of Sales for Satcom and Security, Thales UK

Spoofing, jamming, cyber threats and electromagnetic disruption can down signals and networks before the first shot is fired – rendering forces blind, deaf and outmanoeuvred.

In high-threat theatres, communications availability can determine mission success. Today's military operations demand systems that can adapt, endure and deliver under pressure.

The MOD's Strategic Defence Review calls for an Integrated Force capable of increasing its lethality tenfold across a battlespace in constant flux. That means smarter, more resilient connectivity – not just more of it.

Proposed capabilities like the Digital Targeting Web – underpinned by a resilient network – and the establishment of a Cyber and Electromagnetic Command highlight the growing centrality of this domain to UK defence strategy. But delivering that vision demands communications systems built to operate in congested, complex and contested environments.

SKYNET 6: SatCom as a strategic asset

With the SKYNET 6A satellite scheduled for launch in 2026, MOD's next generation of SKYNET is set for lift-off. This shift repositions SatCom not as infrastructure, but as a strategic

weapon in its own right.

This programme is a complete regeneration of the UK's secure, beyond-line-of-sight comms – spanning the space segment, ground infrastructure and user terminals, prioritising sovereignty, interoperability and modularity across orbits and mission types.

It is one of the MOD's most ambitious efforts to date. Contracts like the Next Generation Land Terminal and the Maritime Military SatCom Terminal offer both challenge and opportunity: to improve the capability of the military's terminals so they advance in step with SKYNET 6's far-reaching ambitions.

Yet beneath this all lies a simple requirement: the frontline operator needs communications that just work – first time, every time.

Hybridisation: adaptable SatCom for today's battlefield

On the frontline, the right message must reach the right person at the right time – regardless of the bearer, and no matter how degraded or contested the environment.

Increasing network hybridisation makes this achievable. By leveraging a combination of orbits (LEO, MEO, GEO and GEO), frequency bands, and non-satellite communication channels (like terrestrial or tactical radio), hybridisation aims to offer the kind of

connectivity operators have come to expect from their personal mobile networks.

Smartphone users don't worry about switching between 4G, 5G or Wi-Fi. The system just connects. That's the ambition for defence. Orchestration is key to delivering this "mobile-like" experience. Whether managed within the terminal or elsewhere in the communications stack. It involves coordinating satellites, frequencies and terrestrial networks to dynamically select the best communication path based on signal strength, latency, bandwidth and security.

Secure data flow is non-negotiable. Every piece of information must be trusted. That means embedding encryption, authentication and integrity measures so data is received without delay, processed confidently and exploited without hesitation.

Civilian telecom standards can't simply be lifted into the military domain. But certain standards can still play a role. 3GPP and Open Antenna to Modem Interface Protocol, and Digital IF Interoperability, for example, can help increase interoperability.

SurfSAT-L: a hybrid solution in action

With hybrid SatCom, capability isn't enough – it has to deliver an effect. Whether enabling machine-to-machine speed communications

for uncrewed systems or accelerating situational awareness, the real test is how information exchange performs under pressure. That means not just roaming networks or resisting interference, but empowering operators with adaptive, secure, mission-ready communications they can trust.

Thales' SurfSAT-L system, selected for the German Navy's F126 frigates, illustrates this approach. It delivers a very high-power tri-band (Ka mil, Ka civil, X) SatCom solution that enables simultaneous transmission on all three bands. The system connects to both MEO and GEO satellites – military and commercial – for optimal connectivity in demanding conditions.

No one system can do it all

Perhaps the most important lesson of all is that no one solution can do it all. No single terminal, radio or satellite can meet the demands of every mission. What's needed is an integrated SatCom enterprise made up of best-in-class tools, terminals, techniques, and methodologies; secure by design, redundancy built in at every layer, with zero single points of failure.

The solution, then, is far greater than the sum of its parts, designed specifically to connect, protect and propel whole teams, from the core to the edge.

A clear vision – and a call to industry

As reaction to the SDR settles, the challenge ahead is becoming clearer. In the words of John Healey, Secretary of State for Defence, "We will give our Armed Forces the ability to act at speeds never seen before – connecting ships, aircraft, tanks and operators so they can share vital information instantly and strike further and faster."

To meet that goal, we need smarter, interoperable systems over siloed kit; solutions developed alongside the customer, rather than designed to meet static, predefined requirements; and a hybrid SatCom enterprise built on the skill, intuition, and ingenuity of industry's many moving, many expert, parts.

The time is now for engineers, suppliers and integrators to seize the opportunity. For comms to go the distance, and for UK MOD to get ahead, industry must get to work – harder, faster and more integrated, not only with each other, but within and between Front Line Commands. ■



Industrial IoT Antenna Solutions must be *Flexible* enough to accommodate different wireless technologies, *Dependable* enough to offer continuous coverage and real-time data and *Tough* enough to withstand harsh weather or rough treatment.

STAY CONNECTED

Improve Your Network Connectivity!

INDUSTRIAL
IOT

MobileMark
antenna solutions

Mobile Mark Antenna Solutions designs and manufactures site, mobile, device, embedded, and covert antennas for 30 MHz – 9 GHz. Applications include GPS Tracking & Fleet Management, Mining, Cellular, 5G LTE, WiFi, ITS/V2X, Public Safety, Military and M2M. Engineering, customisation and bespoke design services are available.

Mobile Mark (Europe) Ltd

Tel: +44 1543 459555

www.mobilemark.com

Email: enquiries@mobilemarkeurope.com

Evolving threats in retail theft require advanced solutions

In recent years, the retail theft landscape has undergone a significant transformation. Organised crime groups now operate with a high level of coordination, approaching theft as a business operation rather than isolated opportunism. These groups often target multiple retail outlets within a single day, focusing on high-value products to maximise profit. This shift has made theft incidents more complex, sophisticated, and challenging to combat.

Confronted with these evolving threats, Dual-Stream recognised the urgent need to rethink their security approach. They aimed to develop solutions that could not only prevent theft effectively but also adapt quickly to the dynamic nature of retail environments. To achieve this, they sought a partner capable of providing secure, scalable, and sector-specific connectivity that could support real-time, high-security theft prevention systems across multiple locations.

Prioritising complete isolation

“Retail theft today isn’t just opportunistic — it’s systematic. The emergence of organised crime groups has fundamentally shifted the landscape, making traditional security measures insufficient,” explains Andy Martin, Business Development Director at Dual-Stream.

The primary technical challenge was to design a network architecture that prioritised security and complete isolation from a retailer’s core infrastructure. This separation was essential to ensure that theft prevention systems could operate independently without exposing sensitive retail data or operational systems to cybersecurity threats. Additionally, the technology had to be highly adaptable to live retail settings, where rapid deployment is often necessary to counteract emerging threats. This meant solutions needed to be implemented swiftly, with minimal disruption to ongoing store operations, and designed around the retailer’s existing operating model — not forcing stores to alter their workflows significantly. Compatibility with diverse retail environments, ease of installation, and future scalability were critical factors that shaped the solution.

To meet these complex demands, Dual-Stream partnered with CSL, leveraging their expertise in IoT connectivity and high-security network solutions.

CSL delivered a comprehensive suite of services, beginning with the deployment of dedicated, secure IoT connectivity tailored for high-security retail environments. A key feature was creating a completely separate network layer that isolated theft detection and prevention systems from the retailer’s main operational infrastructure. This architectural design ensured that sensitive data remained protected and

operational systems remained unaffected by potential cyber threats.

CSL’s infrastructure was built to be scalable and highly resilient, supporting nationwide rollout plans. This was crucial for Dual-Stream’s strategy to expand quickly across multiple locations, ensuring consistent performance regardless of the size or complexity of individual stores. Technical support was integrated throughout the process, with CSL’s sector-specific expertise guiding implementation from proof of concept through to full deployment. The partnership emphasised close collaboration, ensuring that installation processes were smooth, reliable, and minimally disruptive. CSL’s team worked hand-in-hand with Dual-Stream’s IT personnel to tailor solutions that fit seamlessly into existing store operations and could be expanded rapidly as needed.

Martin emphasises that “the real differentiator with CSL is their scalability, robustness, and the partnership we’ve built. They understand their products, our needs, and how to adapt quickly to changing requirements.”

80% loss reductions

With CSL’s support, Dual-Stream achieved a significant breakthrough in retail theft prevention.

The deployment of their solutions resulted in a dramatic reduction in losses

— up to 80% in stores utilising the system. The solutions provided 100% uptime across all deployed sites, demonstrating their reliability in fast-paced, live retail settings. The network’s design prioritised security through complete isolation, preventing potential cyber threats from infiltrating sensitive theft prevention systems. The infrastructure’s scalability allowed for rapid expansion to additional stores without compromising performance or security, enabling Dual-Stream to grow their footprint efficiently.

Throughout the project, CSL’s ongoing technical support played a critical role. Their responsiveness and sector expertise ensured smooth implementation and quick resolution of any issues. The partnership fostered a sense of trust and confidence, empowering Dual-Stream to focus on delivering results rather than troubleshooting technical challenges.

“CSL’s technical support has been vital throughout every phase of the project. From initial proof of concept to full rollout, having a dedicated partner in CSL made a huge difference in our ability to execute quickly and effectively,” says Martin.

By partnering with CSL, Dual-Stream not only implemented an effective theft prevention system but also established a future-proof model rooted in trust, speed, and resilience. This strategy positions them well to stay ahead of organised crime threats and adapt to future security challenges in the retail sector. ■





Upgrading surveillance infrastructure for a leading retail outlet

Located in a bustling shopping district, a prominent retail outlet recognized the critical need to modernize its existing security infrastructure. The primary objectives were to enhance customer safety, effectively prevent theft, and improve operational efficiency. The management engaged the Keep My HomeSafe team to design and implement a customized surveillance system that would meet their unique security challenges and seamlessly integrate with their current operations.

The retail store faced multiple security and operational hurdles. High-traffic areas such as entrances, aisles, checkout counters, storage rooms, and the exterior of the premises required constant monitoring. The existing surveillance setup was

outdated, lacking advanced technological features, which resulted in blind spots, inefficiencies, and potential security vulnerabilities. The client emphasized the importance of incorporating cutting-edge technology into the new system, ensuring compatibility with existing security infrastructure, and minimizing disruptions to daily activities during deployment.

Safeguarding data integrity

Leveraging specialized expertise in retail security systems, Keep My HomeSafe developed a comprehensive, tailored solution. Their approach involved deploying over 40 high-definition

cameras strategically positioned across all critical zones. These cameras provided extensive coverage and included advanced functionalities such as facial recognition, license plate recognition, motion detection, and real-time alerting. This enabled the security team to adopt a proactive stance, responding swiftly to incidents as they occurred.

The system featured centralized monitoring stations equipped with multiple screens, allowing security personnel to oversee various camera feeds simultaneously. To safeguard data integrity and ensure compliance with privacy regulations, Keep My HomeSafe implemented secure storage solutions utilizing encrypted data transmission. This setup facilitated seamless retrieval of footage for investigative purposes. Additionally, a user-friendly interface accessible via mobile devices was integrated, empowering staff to monitor live feeds, review recordings, and manage system settings remotely.

Seamless integration to eliminate blind spots

The Keep My HomeSafe team executed the installation with precision, adhering to industry best practices, client specifications, and regulatory requirements. The process began with configuring a robust and secure network infrastructure, incorporating high-performance switches, routers, and dedicated power supplies to guarantee uninterrupted surveillance. The high-definition cameras, equipped with advanced features, were strategically installed to eliminate blind spots, deter

theft, and bolster overall security.

Seamless integration of the new surveillance system was ensured with existing security components, including access control, alarm, and fire detection systems, creating a cohesive security ecosystem. The deployment was followed by comprehensive testing, staff training sessions, and system audits to verify optimal functionality, user proficiency, and compliance with industry standards.

The deployment resulted in a state-of-the-art surveillance infrastructure that significantly enhanced the retail outlet's security posture. The comprehensive coverage minimized blind spots and allowed for proactive security measures. Advanced features such as facial recognition and real-time alerts enabled swift incident response and facilitated thorough investigations. The mobile-accessible interface provided security personnel with remote monitoring capabilities, increasing operational flexibility. Secure, encrypted data storage ensured data integrity and regulatory compliance, while enabling quick retrieval of footage when needed.

The successful implementation of this customized surveillance system transformed the retail outlet's security landscape. It provided enhanced monitoring, proactive security features, and increased operational efficiency. By leveraging Keep My HomeSafe's technological expertise and innovative solutions, a comprehensive security infrastructure aligned with the client's specific needs was delivered. This upgrade fostered a safer, more efficient, and customer-centric environment, supporting the store's ongoing growth and success. ■

Protect Monitor Control

AKCP

Environmental monitoring experts and the AKCP partner for the UK & Eire.

0800 030 6838
hello@serverroomenvironments.co.uk

Save Energy with AKCP Sensors

Contact us for a **FREE** site survey or online demo to learn more about our industry leading environmental monitoring solutions and how they can help to **reduce your energy costs.**

Server Room environments
Cooling | Power | Fire | Racks | Monitoring



How AI's predictive power can drive data centre sustainability

David Pownall, Vice President, Services, Schneider Electric UK and Ireland

In a world driven by technology, data centres act as the backbone of our information infrastructure. With AI's capabilities growing by the day, and its integration into every aspect of industry growing exponentially, it's no surprise that in order to keep up with accelerated demand, data centres are projected to require \$6.7 trillion capex worldwide by 2030.

In order to power everything from our cloud services to social media feeds, we not only need investment in data centre infrastructure, but also investment into technologies to manage and monitor their energy consumption.

Consuming significant amounts of energy and resources, data centres must integrate sustainability, from design to operation, to ensure operational resilience is up and environmental impact is kept down. Data Centre Infrastructure Management (DCIM) software, and Artificial Intelligence (AI) are two technologies that are set to create more efficient and sustainable data centres in 2025.

Anticipating the scale

A whopping 40 billion devices are projected to be connected to the IoT by 2030. In the face of this demand, resilient datacentres will become strategic imperatives, particularly as AI becomes part of day-to-day business operations.

In fact, three-quarters of data centres currently face increased pressure from AI-driven demands, with only three-in-ten decision makers believing that they are doing enough to enhance the energy efficiency of data centres.

With hypergrowth on the horizon, data centre operators will need new and innovative ways to manage the surge in new devices, ensuring electrical assets are dependable to minimise unplanned downtime.

Keeping cool under pressure

It is imperative that AI data centre growth is decoupled from the environmental impact. For this to be accomplished, low carbon energy sources need to be utilised, new flexible and efficient AI-ready data centre designs must be developed, and sustainable business practices must be put into place. Traditional power and cooling optimisation technologies will need to evolve if they are to support the demands of higher density racks, which accommodate even greater amounts of computing power.

Technologies such as liquid cooling, software-based cooling optimisation, and advanced airflow management are becoming increasingly popular, making it possible to maintain optimal temperatures whilst consuming less energy. With proper airflow management, operators can ensure that cool air is distributed evenly throughout the data centre, preventing hot spots and improving overall cooling efficiency.

Predicting the future is now plausible

It's true that artificial intelligence itself is creating increased demand for data centre infrastructure. However, it could also hold the key to unlocking energy efficiency gains when it is integrated into data centre infrastructure management (DCIM) software,

thanks to predictive monitoring and maintenance capabilities.

When AI is integrated within an infrastructure management system, it collects and analyses data from thousands of sensors, monitoring variables such as temperature, humidity, server loads, airflow, and energy consumption. AI can also learn from external data sources, such as weather data. Instead of controlling cooling based on a fixed schedule, AI aggregates past data and predicted future insights to make adjustments in real time.

This is a gamechanger for data centre operators looking to optimise their resources and prevent existing parts from overheating if a sudden shift in weather, such as a heatwave, occurs. With tools that track energy usage, temperature, and performance metrics around the clock, operators can confidently allocate resources, as well as identify potential areas to optimise energy use.

AI & automation: forecast blue skies ahead

Along with anticipating shifts in temperature, AI algorithms can forecast hardware failures and schedule maintenance before issues snowball, reducing downtime and waste resulting from burnt out parts. By switching to a more proactive approach, operators can keep equipment performant for longer periods of time, prolonging its lifespan and dependability. Proactive asset management is already proving its worth, with some sites reporting reductions in critical asset failure by up to 60%, with maintenance visits only required every five years instead of every three.

AI technologies are also making a significant difference for data centre operators by automating tedious manual tasks, including backup management, load balancing and system updates. Delegating these tasks to AI not only reduces the margin for human error: it also enables operators to focus their energy on more strategic activities which require a more discerning human eye.

AI is also advancing data centre security through tools such as remote management. By deploying cloud-based AI tools, operators can gain visibility across several sites at once: an especially valuable tool for teams working across hybrid environments. These tools offer operators automated alerting should performance deviate from an agreed baseline. Automated alerting not only reduces the likelihood of human error; it also acts as the 'eyes and ears' for data centre operators at any time of day, anywhere. Operators are informed at speed when potential security or equipment issues do arise, so any system vulnerabilities can be addressed in good time, before they impact end-users and services.

A resilient future awaits

The pressure on data centres to deliver sustainable, resilient, and efficient operations will only intensify in the years ahead. To meet these demands, operators can consider AI-driven infrastructure management tools. Remote monitoring, intelligent cooling, and predictive maintenance will all be essential in ensuring consistent, reliable performance as demand continues to soar. Keeping



systems online and fully functional is critical as industries become increasingly reliant on digital technologies. By harnessing AI's full potential, data centre operators

can strike the crucial balance between meeting growing demand and minimising environmental impact, paving the way for a successful digital future. ■

KVM CHOICE

Data Center Solutions Specialists



Secure
Access



Remote
Access



KVM



Extenders



Matrix

Let's talk...
zpe

HASSLE FREE PROCUREMENT OF: IT / POWER / INFRASTRUCTURE EQUIPMENT



Raritan Server Technology ROSE ADDER ATEN mcaB Power nocoSsoTech Smart-AM APC IEC LOCK
 USystems MINKELS Sunbird AUSTIN HUGHES POLIX RNX SPOOK CHIMERA PatchSee zpe

Contact us for immediate quotes:

0345 899 5010 | Sales@KVMChoice.com

KVM | Serial | AV | Matrix | Intelligent Power | DCIM | Racks

AI-ready data centres – preparing for the future

Lauri Salmia, Applied Portfolio Manager, Trane

When it comes to preparing for AI-ready data centres, there is no one-size-fits-all cooling solution. The ongoing revolution in AI, machine learning, and high-performance computing is rapidly transforming data centre operations and demands, changing and placing unprecedented pressure on cooling infrastructure. The diversity of workloads, ranging from traditional storage and enterprise applications to exceptionally high-density AI/GPU compute environments, requires a flexible, scalable approach.

Historically, air-cooled systems have served most data centres well. Air- and water-cooled chillers, combined with new ranges of Computer Room Air Handlers (CRAH) and Fan Wall Units (FWU) have offered robust coverage for facilities with low to moderate server rack densities and remain highly relevant for legacy applications and lower intensity operations also in the future.

However, the surge in AI workloads has resulted in server rack densities which can be tens of times higher than previous generations, which is an obvious challenge for cooling solutions and where traditional air cooling reaches its limits. For this type of server rack densities, liquid cooling solutions are often required. The most common method today is direct-to-chip (DTC) cooling, where cooling

liquid is looped directly via the cold plates of the server racks to remove the majority of the heat. But even in these applications, air-cooling solutions are still needed to reject the remaining residual heat.

Adopting liquid server rack cooling means that chilled water loops can be run at higher temperatures. This significantly increases the potential for free cooling — using ambient air, rather than higher-energy intensive compressor-based cooling. In temperate climates like the UK's, free cooling can be used most of the time during the year and meet big part of the annual cooling delivering significant energy and cost savings.

There are now integrated systems available in the market combining intelligently managed dry coolers and chillers. In this case, mechanical and free cooling part is optimized to minimize the annual energy consumption and data centre PUE (Power Usage Effectiveness) factor. Compared to conventional free cooling chillers, the integrated Chiller/Dry Cooler approach can enable a further double digit reduction in energy consumption without increasing the unit footprint.

Planning for tomorrow

For data centre operators, planning for tomorrow is as essential as meeting today's

requirements. Retrofitting facilities for AI means adopting flexible, modular cooling systems that support both existing and future workloads. Key considerations include:

- **Planning for expansion:** Build in extra capacity and physical space for future increases in rack densities and cooling loads. The ability to scale quickly is crucial, particularly for hyperscale and co-location sites where requirements may change unexpectedly.
- **Embracing mixed technologies:** Get ready to use both air and liquid-cooled systems for current and anticipated future workloads. Trane's comprehensive portfolio allows future proofing your data centres' cooling needs.
- **Maximising energy savings and efficiency:** Global power demand for data centres will grow exponentially in the coming years, and power availability will be one of the bottlenecks for scaling. Big part of the data centre power is used for cooling which means that the future cooling systems needs to be even more energy efficient than today.
- **Proactive heat reuse planning:** Traditionally data centre excess heat has been extracted back to the ambient. This excess heat is a valuable energy

source which can be repurposed and used in many heating applications increasing the total efficiency ratio of a data centre significantly. When constructing new facilities, choosing a location near heat end-users or established infrastructure should be a top priority to make heat recovery viable and economical. For retrofits, it becomes viable to capture and repurpose heat if there are means to physically transport it to the heat end user.

- **Collaboration and circularity:** Partnering with flexible solution providers is critical, whether updating existing systems or building from scratch. A holistic approach, where cooling, free cooling, and heat recovery solutions are all managed under one roof, ensures operators can create a complete circular load system and stop wasting energy.

In summary, operators should avoid rigid, over-specified system designs focused only on present requirements, as well as neglecting heat recovery, especially in regions where infrastructure links to heat end-users can be built or improved at reasonable cost.

Underestimating future demand or ignoring regulatory shifts risks expensive retrofits or loss of competitive edge. ■

PRODUCTS

I The GRC ICeraQ line of liquid immersion cooling systems offers scalable solutions suitable for a wide range of data centre applications, including AI workloads, public and private cloud storage, high-frequency trading, and on-premises infrastructure.

Designed to reduce operational costs, the ICeraQ systems feature a modular architecture with options from compact all-in-one units like the ICeraQ Micro to high-capacity configurations such as the ICeraQ SX and FLEX. These systems support cooling capacities from 45 kW with 32°C water to as much as 368 kW with 13°C water, accommodating diverse density and performance requirements.



The ICeraQ systems deliver significant energy efficiency benefits, reducing cooling energy consumption by up to 90% and lowering server power draw by approximately 11%. They enable high-density layouts and can operate effectively in harsh environments, with deployment times typically around three months. The systems are designed with minimal site requirements and scalable architecture, allowing data centres to grow incrementally and adapt to changing demands while attaining ultra-low pPUE (<1.03).

Built for sustainability and cost-efficiency, ICeraQ liquid immersion units facilitate complete heat recovery and significantly lower carbon footprints. They support deployments in greenfield and retrofit projects, offering up to 30% reductions in upfront infrastructure costs. These systems are ideal for organisations seeking rapid deployment, high performance, and environmental responsibility in their data centre cooling strategies.

I LiquidStack's two-phase immersion cooling tanks offer highly efficient thermal management solutions designed to maximise data centre performance while minimising space and energy consumption. The tanks are available in a variety of sizes and modular configurations, including the DataTank™ 4U for edge and micro data centres, the DataTank™ 48U for full-scale deployments, as well as prefabricated MicroModular™ and MacroModular™ solutions capable of supporting up to 250kW and 1.5MW respectively. Their scalable design enables deployment across a wide range of applications and facility sizes.

The two-phase immersion technology provides industry-leading cooling capacity, outperforming traditional immersion systems by removing up to 30 times more heat per rack. It achieves significant energy

savings, reducing power consumption by approximately 41% compared to air cooling, and lowering CAPEX by 44%. Additionally, it creates space savings of up to 59% in white space, while offering a total cost of ownership (TCO) improvement of around 15% over 20 years. The systems support chips rated up to 1,000W, with advanced flow technology that optimises heat transfer and rejection, enabling as low as 1.02 pPUE.

Designed for high-performance applications such as AI, HPC, cloud services, cryptomining, and edge data centres, LiquidStack's two-phase systems provide extreme cooling power in a safe, flexible, and future-proof package. Their modular form factors allow easy scaling and rapid deployment, making them suitable for hyperscale, enterprise, and high-density environments seeking maximum efficiency and space savings.

I The DCX Standard Server Immersion Enclosure is designed to support standard 19" or 21" servers, allowing for seamless integration within existing data centre infrastructure. It features an immersion depth of 850mm, enabling efficient heat transfer of 61-70 kW depending on configuration. The system offers a power density of approximately 3.6-4 kW per IRU, supporting up to 20 rack units (RU) or 40 multi-node servers, with the capacity to deliver 2-3 times more compute density per rack compared to traditional cooling methods.

Constructed to fit within the dimensions of a standard 600x1200 mm rack, the enclosure supports single or dual-level configurations for deployment flexibility. It includes a hydraulic compartment with built-in high-capacity heat exchangers and 2N redundant

pumps, ensuring continuous operation and reliable heat exchange. The system's design facilitates easy access to critical components such as pumps and heat exchangers, simplifying maintenance and reducing potential downtime.

The system employs large plate heat exchangers and dedicated immersion tanks, which can be stacked in two or three levels. These tanks are equipped with temperature sensors that provide real-time data on fluid and primary loop temperatures, enabling precise thermal management. The design emphasises energy efficiency, with the ability to recover heat fully and operate at significantly reduced energy consumption compared to traditional air-cooled solutions. Overall, the enclosure supports high-density server deployment while maintaining operational reliability.



I JetCool's Direct-to-Chip Liquid Cooling offers a cutting-edge solution for modern data centres facing increasing heat loads from AI and high-performance computing (HPC). As CPUs and GPUs grow more powerful, traditional air cooling becomes insufficient, leading to inefficiencies and thermal bottlenecks.



Designed for high power density devices, JetCool's patented microconvective cooling technology eliminates thermal pastes and interface materials, reducing thermal resistance and boosting performance. This scalable solution can cool devices from 150W up to over 2,000W, making it ideal for next-generation chipsets and demanding workloads. Data centres using JetCool achieve over 80% performance improvements compared to conventional air cooling, while AI applications benefit from stable, efficient operation without costly refrigeration cycles.

Beyond performance, JetCool's cooling modules promote reliability and sustainability — reducing cooling costs by 18%, allowing higher coolant temperatures, and eliminating water consumption. With easy integration and future-proof design, JetCool empowers organisations to operate devices safely and efficiently, supporting growth in AI, HPC, and advanced semiconductor development. Transform thermal management and unlock new levels of compute performance with JetCool's proven liquid cooling solutions.



Please meet...

George Ashwin, Channel Director, AddOn Networks

What law would you most like to change?

One thing relevant to the work I'm doing at the moment with AddOn Networks is the forced labour that still takes place within supply chains across the United Kingdom. We're seeing other countries within the European Union action robust human rights laws that protect workers and hold corporate entities to account. Yet over here, people who have experienced forced labour don't get the support they deserve.

I would say we need to replace some of the outdated human rights legislation with new rules. These would place increased pressure on businesses to create safer workplaces and ensure they are constantly demonstrating they are not involved in labour abuses.

Who was your hero when you were growing up?

Many people may mention a parent or a teacher, but in actual fact my hero was James Hetfield, the lead singer and guitarist from Metallica! That band definitely inspired me to learn an instrument, and I still play the bass today.

What was your big career break?

I would have to say it's when I joined the AddOn business back in 2018. I'd held a few roles before starting with the company, including a three year stint with the Cotswold District Council as a Customer Service Advisor. However, as soon as I got the job as an Inside Sales Representative at AddOn, I was able to hit the ground running.

Since day one, I've had the support and opportunities to keep progressing. Now, as a Channel Director, I have the opportunity to work on some exciting projects with some of the leading businesses across EMEA.

What did you want to be when you were growing up?

Growing up I always wanted to be either a marine biologist or a Naval officer. Something related to the sea at the very least! For three years between 2010 to 2013, I did get the opportunity to be a Midshipman for the Royal Naval Reserves, which my younger self would be very happy to learn, I'm sure.

The Rolling Stones or the Beatles?

For me, it has to be the Rolling Stones.

If you could dine with any famous person, past or present, who would you choose?

It would definitely have to be a historical figure – I have a degree in Ancient and Medieval History from the University of Birmingham, so it'd be good to put some of my knowledge to good use! I've always enjoyed learning about how people in the past lived, worked, traded and enjoyed their leisure. Let's say Marcus Cicero, the Roman statesman. He's someone who interests me greatly.

What's the greatest technological advancement in your lifetime?

It would have to be the full-scale deployment of the internet. The way it expanded and evolved over such a short period of time to what it is today is incredible, and now we live in a society that is totally dependent on it for business, leisure and beyond. It's

also been the great enabler for other game changing technologies since its inception.

What would you do with £1 million?

If I ever got that much money, I would look to buy some land and build my own cottage in the Cotswolds. I was born and raised there, and for my money, it's the best part of the United Kingdom. Back in the day I was a Venturer for Raleigh International, and part of the work I was doing over there included building a

community hall – maybe I could apply some of those skills to building a house? Of course, knowing the cost of living down there I'll definitely still need a mortgage!

What's the best piece of advice you've been given?

One thing that always sticks with me is 'don't ask others for anything you wouldn't be prepared to do yourself'. It's something I've tried to stick to throughout my career so far.

If you had to work in a different industry, which would you choose?

I think I would join the Navy – it's always been of interest to myself, and as I mentioned, I was previously a Navy reservist.

Where would you live if money was no object?

I feel I may have already given my answer away on this one... it'd still have to be the Cotswolds for me. I've been lucky to visit a number of different countries in the last few years, but there's no place like home really. ■

SAVE THE DATE

DATA centres

Ireland

RDS, Dublin: 19-20 Nov 2025

Infrastructure • Services • Solutions

DataCentres Ireland combines a dedicated exhibition and multi-streamed conference to address every aspect of planning, designing and operating your Datacentre, Server/Comms room and Digital storage solution – Whether internally, outsourced or in the Cloud.

DataCentres Ireland is the largest and most complete event in the country. It is where you will meet the key decision makers as well as those directly involved in the day to day operations.

Entry to ALL aspects of DataCentres Ireland is FREE

- Market Overview
- Power Sessions
- Connectivity
- Regional Developments
- Heat Networks and the Data Centre
- Renewable Energy
- Standby Generation
- Updating Legacy Data Centres

Meet your market

Headline Sponsor

Ticket & Registration Sponsor

Lanyard Sponsor

For the latest information & to register online visit

www.datacentres-ireland.com