

IN DEPTH:  
SD-WAN  
P7-8



Data centre optimisation

Priorities for infrastructure for 2026 and beyond

Dean Boyle,  
EkkoSense, p5



The next risk for tech leaders

A shrinking talent pipeline threatens the UK ecosystem

Imran Akhtar,  
mthre, p14



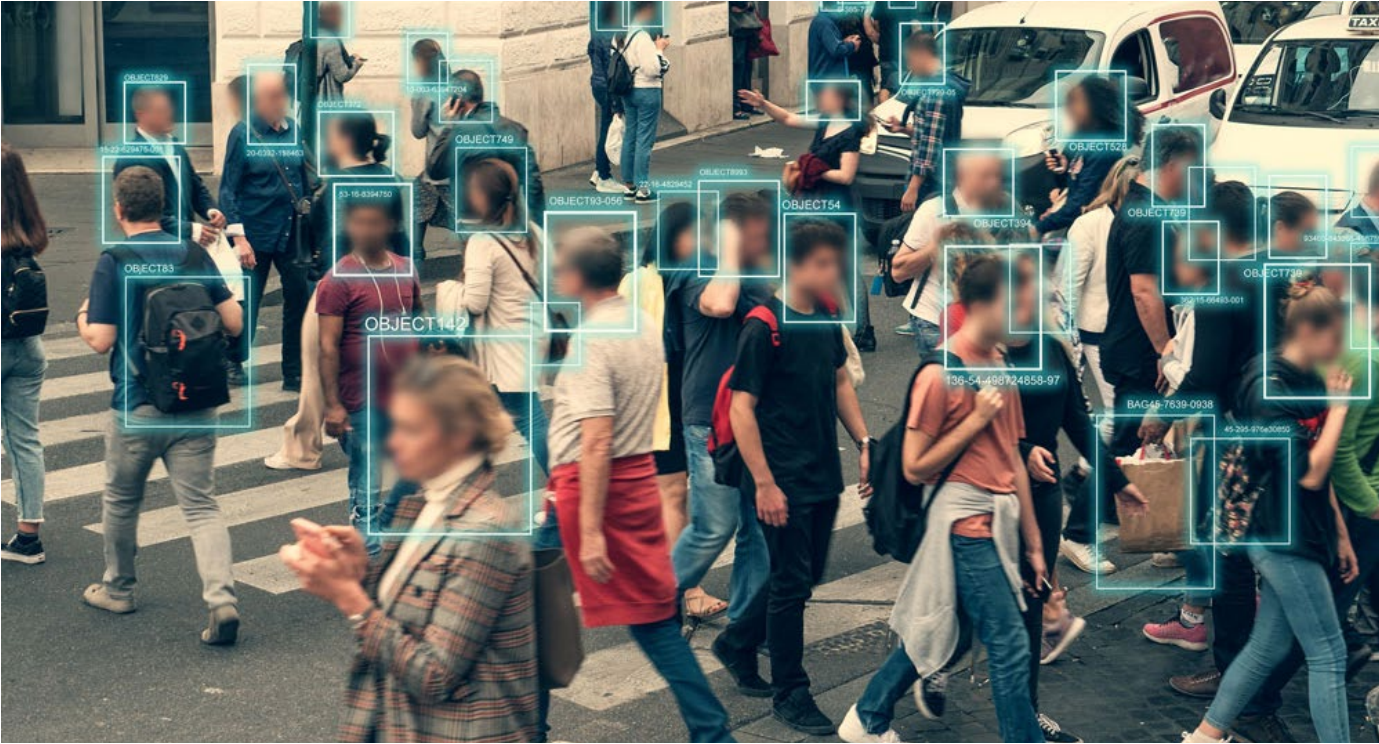
Questions and answers

As a child, I was fascinated by Indiana Jones

Matthew Thompson,  
Airsys, p16



Budgeting for the AI boom



Late in November, the long-awaited Autumn Budget finally landed, outlining a series of major moves from UK Chancellor Rachel Reeves as the government seeks to sharpen the country’s competitive edge.

Central to the announcement were fresh investment plans targeting high-growth industrial sectors, including the launch of two AI-focused growth zones in Wales — initiatives projected to generate more than 8,000 new jobs and stimulate broader regional innovation.

Reeves also stressed the importance of strategic public spending in building the industries of the future. A key shift came with the confirmation that government procurement rules have now been updated to allow the UK to “buy British” where national security is at stake, a change she positioned as vital for rapidly advancing fields such as AI.

So how is the industry viewing the Budget’s AI ambitions?

According to John Lucey, VP EMEA at Cellebrite, the pressure on public-sector organisations, and policing in particular, is becoming increasingly acute as demand for faster case resolution intensifies: “the tidal wave of AI isn’t slowing down and for public sector organisations, particularly police forces, there is a growing pressure to reduce time to evidence. To achieve this, AI and automation are essential to streamline

time-consuming tasks such as reporting and data analysis to save hours and millions in efficiency. Especially when connected to public safety, AI always needs human verification and oversight,” he notes. “People must be the ones to govern AI’s use cases, using it as an assistant to speed up otherwise menial and manual tasks. For policing, this means digital forensics teams can leverage AI to shorten case times through content classification, evidence prioritisation and automated device extraction to expedite verdicts.”

Others argue that the Budget highlights the right intentions, but that ambition needs to be matched with serious investment in the country’s digital foundations.

Stuart Harvey, CEO of Datactics, stresses the importance of strengthening the systems underpinning AI adoption: “AI is revolutionising public services to drive greater efficiency, innovation and economic growth, but to fully harness these advancements, the UK must prioritise strategic investment in data infrastructure and the responsible deployment of AI. Without robust systems to manage, analyse, and secure data, businesses and government departments risk falling behind in an increasingly competitive global market,” he says. “A strategic investment in data governance will help boost productivity and ensure the UK remains at the forefront

of the AI boom while ensuring economic stability and long-term prosperity.”

Meanwhile, concerns remain about whether the UK’s physical and digital infrastructure is prepared to support the scale of AI-led growth the Budget envisions. Matt Hawkins, Founder and CEO of CUDOCCompute, cautions that progress depends on getting the fundamentals right.

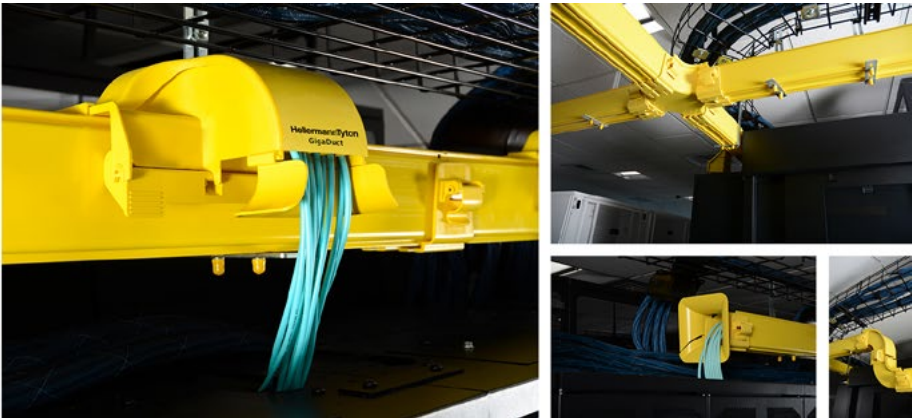
“The OBR’s outlook shows the UK growing at around 1.5% a year, which means every plan for innovation needs a practical foundation. AI driven growth can only happen when the underlying infrastructure behind it is strong, sustainable and ready to scale. That means having reliable, sovereign compute capacity and clean, affordable power to drive it – which has been a key blocker to date,” says Hawkins. “If these zones are going to deliver the impact the Chancellor is banking on, we need to match investment in innovation with the energy and digital infrastructure that supports it. Backing renewables and future proofing compute is how we turn ambitious Budget goals into real economic progress.”

Together, these perspectives paint a picture of cautious optimism: the Budget sets a bold direction, but the UK’s ability to deliver on its AI promises will depend on whether practical foundations keep pace with political ambition. ■

GigaDuct  
Fibre Raceway

Revolutionise how you manage and safeguard your critical infrastructure.

HellermannTyton





## Birmingham City University partners with North for £1 million smart access control system

Birmingham City University (BCU) has awarded North a £1 million contract to install a state-of-the-art access control system as part of its initiative to become a smarter campus.

This investment marks BCU's initial step toward enhancing campus security, sustainability, and the overall student experience. After a competitive tender process, North will design and implement an innovative security solution utilising Genetec technology to replace the university's aging current system.

BCU, one of the UK's largest and most diverse universities, is home to over 31,000 students from more than 100 countries. The upgrade will be rolled out across its two city centre campuses, impacting thousands of students, staff, and visitors. The new system aims to future-proof the university's infrastructure by ensuring resilience, regulatory compliance, and improved safety standards.

The upgrade will enable BCU to transition to a digital, app-based access control system, aligning with its sustainability objectives. The university, recognised as Birmingham's most sustainable institution and among the UK's leading environmentally conscious universities, aims to leverage this technology to support its green goals.

North's integrated solution will seamlessly connect the new access control platform with existing systems such as student records, streamlining operations and bolstering security. Additionally, the system will generate valuable data and analytics, offering insights into areas like student accommodation occupancy and attendance patterns, aiding staff in operational decision-making.

"It is fantastic to partner with BCU on its journey toward becoming a smart campus. This upgrade not only enhances security but also provides a modern, user-friendly experience for students and staff."



As higher education budgets become more constrained, adopting smart technology is essential for future-proofing campuses and creating safer, more sustainable learning environments," said Andrew Foster, Managing Director for Public Services at North.

The new access control system will also help BCU comply with emerging legislation, including Martyn's Law, ensuring safety standards are met and maintained.

"This partnership with North reflects our commitment to building future-ready campuses. We're not just upgrading security; we're reimagining how people move through and interact with our spaces. North's expertise will accelerate our transition to a smart, data-driven environment that supports sustainability and enhances safety," said Nick Moore, Director of IT and Digital at BCU. ■

## Cumbria Police boost crime fighting with advanced vehicle connectivity from Ericsson

Cumbria Police Force has taken a major step forward in its digital policing capabilities by partnering with Ericsson and Axon to deploy cutting-edge cellular connectivity in over 50 police vehicles.

Using the Ericsson Cradlepoint R1900 router, this initiative delivers reliable, high-speed mobile data connectivity, enabling officers to access live information, share real-time intelligence, and respond more effectively to incidents across the vast county.

Policing today heavily depends on data from laptops, smartphones, and various body and vehicle-mounted cameras. Thanks to Axon's connected ecosystem — including Axon Evidence and Axon Fusus — these tools are now integrated into a seamless, interoperable network that enhances decision-making and officer safety. However, challenging geography and outdated infrastructure previously limited network coverage in some areas, hampering frontline response and operational efficiency.

The installation of Ericsson's R1900 routers has transformed this landscape. By integrating live data streams into the Axon platform, connectivity has become more stable and widespread. One key example is the enhanced use of Automatic Number Plate Recognition (ANPR) cameras mounted on police vehicles, which now automatically flag vehicles of interest regardless of location. This allows officers to focus on actual threats rather than routine stops, increasing operational precision.

The impact is especially evident during large-scale events such as Appleby Horse Fair, which attracts tens of thousands of visitors annually. As one of the UK's smallest police forces in terms of staffing but one of the largest geographically, Cumbria Police must operate efficiently and strategically. Since deploying the Ericsson and Axon solutions, officers

have been able to identify high-risk individuals proactively and monitor live intelligence throughout the event. In 2024, this approach contributed to the arrest of 123 people — more than double the previous decade's average — and a notable rise in Traffic Offence Reports from 220 in 2023 to 377 in 2025, thanks to connected vehicle cameras.

"Ericsson's in-vehicle routers have been a game-changer, providing officers with real-time intelligence and enabling more precise, proactive policing. This has made Cumbria a less attractive place for criminals and boosted morale among frontline responders. Our commitment to delivering outstanding service is supported by these technological advances, helping us protect communities more effectively," said Chief Inspector Lee Skelton.

Graham Everington, Ericsson's Sales Manager for the Public Sector, emphasized the importance of dependable connectivity for emergency responders, noting that "reliable, high-speed networks are vital for emergency services to perform their duties effectively. We're proud to support Cumbria Police's mission and look forward to further collaborations to enhance community safety."

"Supporting Cumbria Police with real-time data integration is a testament to how connected technology improves response times, collaboration, and officer safety. By embedding live video and alerts into the Axon ecosystem, we're helping officers serve communities faster and more securely," said Alex Lowe, Senior Director of Sales at Axon for UK and Ireland.

This innovative partnership demonstrates how reliable cellular connectivity and integrated digital tools are reshaping law enforcement, making policing more proactive, efficient, and community-focused. ■

## Most in-house IT projects abandoned due to hidden costs and risks

Exclaimer has unveiled the findings of its 2025 'Build vs. Buy: The True Cost of DIY IT Solutions' report, offering a comprehensive look at how global IT and security leaders are reevaluating the real costs, risks, and benefits of developing software internally versus purchasing from trusted vendors.

Based on insights from over 2,000 decision-makers, the report highlights a striking trend: 71% of in-house-developed projects are eventually abandoned. Dubbed 'The DIY Mirage,' this phenomenon exposes the illusion of control and efficiency that diminishes as maintenance burdens, compliance challenges, and long-term costs escalate.

The research also uncovers regional differences: in the UK, 33% of teams build in-house primarily to meet compliance and data residency requirements, while in the US, 28% do so mainly to integrate with legacy systems. However, this pursuit of speed often leads to higher costs and operational issues, with US IT leaders reporting a 74% downtime rate from internal tools compared to 50% in the UK.

"Every IT leader faces the question: do you build or do you buy? The data shows

that while building in-house may seem like maintaining control, it often comes at the expense of time, security, and scalability. We've seen how operational burdens can quickly overwhelm teams when they're forced to maintain tools that were never designed to scale. This research provides organisations with a clear view: true efficiency isn't about owning every line of code, but about freeing teams to focus on growth and innovation," said Paul Hammond, Chief Product & Technology Officer at Exclaimer.

The report underscores a widening gap between perceived efficiency and actual outcomes. Despite nearly half of IT teams preferring to develop their own tools, only 8% of these projects are delivered on time, and just 11% remain within budget. In reality, over half take 1.6 to 2 times longer than planned, and 46% of projects end up costing nearly twice their initial budget.

Furthermore, ongoing maintenance demands are significant: 63% of teams spend between 10 and 50 hours monthly maintaining internal tools, while 66% spend an additional \$20,000 to \$100,000 annually just to keep systems operational. Security concerns are also prominent,

with 64% reporting security-related downtime and 31% citing compliance and data protection as major barriers. This transforms what may have started as a cost-saving initiative into a long-term liability.

A startling 71% of IT and security leaders admit to building tools internally only to abandon them later, with the figure rising to 81% among CIOs and 73% among CTOs. Despite confidence in their own builds — 59% of US leaders believe they offer better protection — downtime remains a universal challenge, underscoring the risks of DIY approaches.

The report highlights a clear industry trend: organisations are increasingly turning to specialised vendors. When

asked why they prefer buying over building, 30% of IT leaders cited faster deployment, 29% pointed to access to expertise, and 28% emphasised reliability.

Regional differences influence this shift. UK teams, driven by regulatory pressures (33%), lean towards vendor solutions to ensure compliance and control. Conversely, US teams, traditionally focused on speed (23%), are now embracing vendor partnerships for quicker scalability and reduced maintenance burdens. Overall, the trend indicates that buying from trusted providers now outweighs building for control, as organisations prioritise efficiency, security, and predictable performance. ■

### EDITORIAL:

**Editor:** Amy Saunders

**Designer:** Ian Curtis

**Sub-editor:** Gerry Moynihan

**Contributors:** Dean Boyle, Renuka Nadkarni, Nick Rogers, Pejman Tabassomi, Will Hitch, Imran Akhtar, Stephen Patrick, Matthew Thompson

### 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, IC113, 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

# Renewable Energy Association launches data centre coalition

The Renewable Energy Association (REA), a UK-based non-profit trade organisation, has launched its new Data Centre Coalition to drive the development of clean, scalable power sources for the UK's data centre industry and to shape relevant policy frameworks.

The coalition aims to foster investable clean-power models, establish an integrated national planning approach, create policy certainty, and provide evidence-based input to government and regulators.

The coalition's founding members include industry players such as Enfinium, Greenscale, Apatura, and Clarke Energy.

"With 400 members, we recognised the need to act at this pivotal moment. The UK is competing globally to attract data centre

investment and meet the sector's rapidly rising energy demand while addressing broader sustainability challenges. Our Data Centre Coalition gives us the collective strength to engage directly with government decision-makers, ensuring that policies are informed by the expertise of those delivering the infrastructure vital to the UK's digital and economic ambitions," said REA CEO Trevor Hutchings.

The UK is positioning itself as a leading hub for data centres and artificial intelligence innovation. However, recent reports project that the country's data centre electricity demand could increase by 200-600% between 2025 and 2050. Concerns remain over whether the UK's current generation capacity and

grid infrastructure can support such exponential growth.

National Grid, the UK's transmission operator, has reported a surge in data centre connection requests, which now account for over half of the 19GW of load seeking connection by 2031. Projections indicate that data centres could consume up to 9% of the country's electricity demand by 2035, compared to 2.6% today.

Last year, the UK government's National Energy System Operator (Neso) released the Clean Power 2030 report, outlining a pathway to develop a fully integrated, low-carbon power system by that year capable of supporting a fourfold increase in data centre energy use. The report envisions offshore wind making

up over half of the UK's electricity generation, with solar contributing nearly 30%. It also highlights other low-carbon technologies like hydrogen and carbon capture and storage (CCS) to enhance system resilience. Despite these plans, questions remain about whether renewables alone can provide a reliable backbone for the energy system.

To ensure baseload capacity, the UK has increased investment in nuclear power. Notably, Rolls-Royce is developing a 470MW small modular reactor at Wylfa in Wales, marking the UK's first site dedicated to this type of advanced nuclear technology, which promises to provide a reliable, low-carbon energy source to support future data centre growth. ■

## DSIT explores £250 million cloud contract

The UK Department for Science, Innovation, and Technology (DSIT) has begun a preliminary market engagement process to procure cloud computing capacity aimed at expanding the nation's artificial intelligence (AI) capabilities.

As detailed in an engagement notice, the eventual contract could be worth up to £250 million over four years.

The goal of this procurement is to enhance the existing "AI Research Resource" (AIRR), which is currently supported by two supercomputers: Isambard-AI, operated by HPE in partnership with Nvidia and the University of Bristol, and Dawn at the University of Cambridge. The selected cloud provider will need to seamlessly integrate with the AIRR Portal — either through a multi-cloud approach or direct provision — to ensure smooth access to AI resources.

DSIT has outlined three key objectives for the contract: to increase the UK's AI capacity twentyfold by 2030, to ensure AIRR users have access to the most advanced hardware in a timely manner, and to provide facilities that will accelerate innovation across critical sectors such as climate science, energy, medicine, and advanced materials.

In addition to expanding GPU capacity, the contract requires a managed service offering secure data storage, orchestration for machine learning workloads, usage monitoring, reporting, demand forecasting, and active security management.

The anticipated contract duration is from May 2026 to March 2030, with interested parties invited to register their interest by 15 January 2026.

The UK's current supercomputing infrastructure includes Isambard-AI, launched in July 2025 as a £225 million, 5MW supercomputer built by HPE and Nvidia at the University of Bristol, delivering 23 exaflops of AI performance and ranking 11th on the latest Top500 list. Dawn, located at the University of Cambridge, ranks at number 92 with 53.85 petaflops of peak linpack performance.

The UK's Isambard-AI launched back in July. A 5MW, £225 million supercomputer, it was built by HPE in partnership with Nvidia and the University of Bristol. It boasts 23 exaflops of AI performance (278 petaflops peak linpack). ■



**ELEVATE**  
Future Faster

## The future is fast


As density and performance requirements escalate, your infrastructure must elevate.

White space redefined: Elevate fibre, intelligent racks, smart power, DCIM, containment and liquid cooling.

High Density Fibre Connectivity   Racks and Containment   Fibre Duct   iPDU



Explore the portfolio:  
[elevate.excel-networking.com](https://elevate.excel-networking.com)

 an excel solution



## GigaDuct Fibre Raceway

- Made in Britain
- Built for Speed
- Designed for Data Centres

In today's data-driven world, the infrastructure behind our digital experiences is evolving rapidly. From cloud computing to AI workloads, data centres are under pressure to deliver faster, more reliable performance - and that starts with how fibre is managed. One often overlooked but critical component is the fibre raceway system: the structured pathway that protects and organizes fibre optic cabling.

HellermannTyton's GigaDuct Fibre Raceway System is engineered to meet the demands of high-density, high-performance environments. Whether you are a data centre manager, IT decision-maker, or network engineer, understanding the role of fibre raceways - and choosing the right one - is essential to futureproofing your infrastructure.

### GigaDuct - Designed for Speed, Simplicity, and Strength

HellermannTyton's GigaDuct Fibre Raceway System stands out for its true tool-free coupler - a major differentiator in a market where many "tool-free" claims still require some manual adjustment, clips, nuts 7 bolts, or specialist tools. GigaDuct's tool-free coupler enables genuine push & grip assembly, making it the fastest fibre raceway system to install on the market today.

Its modular design, wide range of transitions, accessories and comprehensive mounting options supports custom routing both overhead and underfloor installations.

Key benefits include:

- Rapid deployment with no tools required for coupling or creating cable drop off points.
- Fire-retardant materials that meet stringent safety standards.
- Compatibility with other HellermannTyton fibre systems for seamless integration. Such as our high-density RapidNet Ultra Solution.

Whether you are upgrading an existing facility or building from the ground up, GigaDuct offers the flexibility and reliability needed to support mission-critical operations.

### Ready to Upgrade Your Fibre Management?

Whether you're planning a new deployment or optimising an existing setup, the GigaDuct Fibre Raceway System offers a smarter, safer, and more scalable way to manage fibre. With proven performance, unmatched installation speed, and lifetime support, it's the choice of professionals who refuse to compromise on service, quality and reliability.

**HellermannTyton**  
**GigaDuct**

## Cellnex UK and Harrow Council to enhance mobile connectivity

Cellnex UK has announced a new partnership with Harrow Council in London to deploy Small Cell technology throughout the borough.

The initiative aims to address mobile connectivity blackspots around busy high streets and transport hubs by installing small, shoebox-sized base stations on street furniture such as lampposts, CCTV poles, and old payphone kiosks. These Small Cells deliver targeted coverage of up to approximately 100m, making them ideal for dense urban environments where reliable 4G and 5G connectivity is essential.

Cellnex UK has previously collaborated with councils in Hounslow and Swansea on similar projects, and their expansion into Harrow indicates that these efforts are showing promising results. The Small Cells are designed to be open access, allowing any mobile operator to utilise them at wholesale once they are installed, fostering a more competitive and comprehensive mobile network.

"Reliable 4G and 5G is no longer a luxury but a necessity. We know it can be frustrating trying to use data or connect to mobile signal in busy areas. That's why we're putting residents and businesses first by bringing better connectivity to help people carry out their day-to-day activities while on the go. This partnership helps to deliver Harrow's Digital Infrastructure Strategy, which aims to support the rollout of advanced mobile networks and full-fibre broadband to foster economic growth, boost digital inclusion, and attract private investment," said Councillor Norman Stevenson. ■

## UK organisations fail to fully backup sensitive data

According to new research from Cohesity, nearly one-third (31%) of organisations in the UK do not back up all their critical data, leaving them vulnerable to operational disruption in the event of a cyberattack.

While UK companies are increasingly aware of the importance of threat detection and response, data protection and recovery efforts remain fragmented, creating significant challenges. For instance, 38% of organisations do not apply consistent backup controls and policies across all locations, which creates gaps in protection.

Furthermore, nearly half (45%) of organisations do not back up all workloads uniformly, including virtual machines, applications, and unstructured data. This inconsistency makes it difficult to recover data efficiently when needed. Additionally, only 45% follow the fundamental '3-2-1' backup rule - maintaining three copies of data on two different media types, with one stored off-site - leaving many vulnerable to data loss.

The report also highlights that less than half (45%) utilise immutability features across all backup data to prevent cybercriminals from altering or deleting backups, risking the integrity of their recovery points. ■

## Slough approves major data centre at former paint factory

Slough Borough Council has granted outline planning permission for a significant data centre project on the site of a former paint factory off Wexham Road.

The development, proposed by Equinix, plans to utilise approximately half of the historic AkzoNobel site for large warehouse facilities to support various digital services. While the council approved the outline, details regarding the building's appearance, scale, and landscaping will be addressed in a subsequent application.

The local authority sold the site to Equinix in 2022 for £143.75 million as part of efforts to reduce its substantial debt. The council had initially purchased the land in 2021 with plans to develop 1,000 homes there. However, developers have

indicated that sufficient power supply for the later stages of the project may not be available until 2038.

A portion of the former AkzoNobel site is already being used for data centre development. Additionally, a public inquiry was recently held to consider whether a major data centre should be constructed elsewhere in Slough, specifically on a 20.2-acre green belt site known as Manor Farm Propco Limited. The company has applied to develop the site with a data centre, Battery Energy Storage System (BESS), generators, and other infrastructure. The final decision on this proposal will be made by the Secretary of State for Housing, Communities and Local Government in the coming months. ■



## Half of government CIOs expect increased IT budgets in 2026

More than half of government Chief Information Officers (CIOs) anticipate their IT budgets will rise in 2026, driven by increasing demand for artificial intelligence (AI) and other digital technologies despite ongoing fiscal constraints, according to recent industry research.

A survey of 284 government CIOs revealed that 52% expect specific budget increases for AI and related innovations, underscoring a continued commitment to digital transformation within the public sector.

Key investment priorities include cybersecurity, which 85% of CIOs identified as a top area for funding, followed by AI and generative AI at 80%, and cloud platforms at 76%. The data suggests that governments remain focused on digital initiatives that can deliver measurable improvements in public

service delivery. CIOs are under pressure to justify expenditures by demonstrating how technology projects align with mission objectives such as cost savings and enhanced user experiences.

A significant 74% of government CIOs reported that they have already deployed or plan to deploy AI solutions within the next year. Interest in generative AI is particularly high, with 78% indicating current or imminent deployment plans. Nearly half (49%) also plan to introduce AI agents, such as digital assistants, in the coming 12 months.

Boosting internal productivity is the leading priority for government CIOs in 2026, with 51% focusing on increasing employee output. Launching new digital products and services ranks second at 38%, closely followed by efforts to enhance citizen experience at 37%. ■

### Word on the web...

## Building the trusted backbone for the AI era

**Renuka Nadkarni, Product Officer, Aryaka**

To read this and other opinions from industry luminaries,

visit [www.networkingplus.co.uk](http://www.networkingplus.co.uk)







# Keeping pace with AI: data centre optimisation priorities for 2026

Dean Boyle, CEO, EkkoSense

Today's data centre leaders face an unprecedented range of operational challenges. Traditional goals such as reducing thermal & power risk and supporting digital transformation initiatives are still critical. However, as we enter 2026, data centre operations teams are already pretty much maxed out with the introduction of AI/HPC and liquid cooling infrastructure, while also faced with the need to unlock carbon savings as part of corporate net zero programmes and initiatives.

Addressing these activities in parallel can lead to potentially conflicting concerns. Businesses are under pressure to build AI functionality into their operations yet introducing and supporting the latest AI infrastructure can place huge pressure on data centre resilience and availability. At the same time, data centre operations are searching for ways to reduce energy usage and secure quantifiable carbon savings while simultaneously delivering against growing data centre workloads.

It's a complex balancing act, demanding a comprehensive and sustained commitment to optimising all aspects of performance. Achieving requires new levels of insight into existing thermal performance, power provision and capacity management – levels of insight that simply cannot be achieved by relying on traditional legacy Data Centre Infrastructure Management (DCIM) and Building Management System (BMS) tools.

## The visibility gap

Relying on a typical BMS view means that most data centre teams still only see their cooling unit temperatures. Rack inlet temperatures are largely unmonitored, meaning that their true status is effectively invisible. Only a small percentage of data centre M&E teams actually monitor and report equipment temperatures on a rack-by-rack basis; most data centre operations remain in the dark when it comes to effective performance optimisation.

Because of this, it's not unusual to find expensive power and cooling resources that are being used inefficiently. This lack of real-time insight into actual data centre cooling, power and capacity performance means that operations teams often have to over-cool because of this uncertainty.

## Making optimisation smarter

In our research we found that current average data centre cooling utilisation stood at just 40% – implying that significant cooling capacity was effectively stranded as nobody knew how to release it and apply it elsewhere. Even the best run data centres still have cooling, power and capacity challenges. Put an effective data centre optimisation programme into place though, and you can reduce your cooling costs by up to 30%.

However, it's not only the ability to deliver quantifiable energy and carbon savings that makes such a difference. Effective capacity planning helps you to quantify your true cooling capacity – and potentially stop unnecessary and significant spending on new cooling systems. Unlocking stranded capacity lets operations run their data centres leaner – translating directly into the kind of CO2 and cooling energy usage reductions that helps teams to reduce Power Usage Effectiveness (PUE) scores and support sustainability goals.

## AI takes DC efficiency further

Taking advantage of the latest AI and machine learning capabilities enables data centre

teams to take performance optimisation to the next level. Automated PUE and embedded ESG reporting can free valuable operations resources to focus on added value activity. Real-time visibility helps operations teams answer the key engineering questions that need answering before simply deploying liquid cooling – including establishing the exact blend of air and liquid cooling technologies needed within the same room.

As organisations work to make their data centre operations as efficient as possible, AI-enabled optimisation tools can also be deployed to ensure that that rooms continue to optimise

cooling delivery. AI Advisory tools continuously learn about a specific cooling unit's operation, and provide immediate advice on performance enhancements such as cooling unit changes or liquid cooling efficiency.

## From reactive to proactive

Similarly many data centre teams are now taking advantage of advanced anomaly detection so that they can focus in on any drift from control set-points. They can then use the data collected from equipment such as CRACs to alert any abnormal changes in

performance. Rather than wait for traditional approaches such as BMS monitoring to provide an alarm, this kind of anomaly detection can pick up on potential issues – and give the operations team time to resolve them – before they become critical.

This level of continuous innovation is essential if organisations are committed to making their data centre operations as efficient as possible. Unlocking incremental cooling, power and capacity efficiencies needs to be business-as-usual for data centre teams as they work to keep their PUE scores on a downward trajectory. ■

**APC**

Uninterruptible Power...

# REDEFINED

The future of uninterrupted 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 uninterrupted 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](http://www.apc.com)

Life Is On | **Schneider Electric**



# Server security must-knows



**Nick Rogers, CEO, Exacta Technologies**

In today's digital-first economy, server infrastructure is no longer a background function. It forms the foundations on which organisations operate and innovate.

Many UK organisations have developed exceptional software platforms, often built with remarkable technical depth. A significant number continue to run these workloads on established on-prem estates. This isn't resistance to change; it reflects the ongoing need for sovereignty, regulatory control, predictable performance, and infrastructure that stays physically close to the business. For many mission critical workloads, on-prem environments remain the most reliable and strategically aligned choice. But as software evolves, infrastructure must evolve with it to avoid becoming a constraint.

Meanwhile, the threat landscape is accelerating. Ransomware, firmware exploitation, and supply chain vulnerabilities increasingly target the underlying layers of enterprise systems. With AI sharpening the precision of attacks, traditional software-only tools can struggle to keep up.

## A hardware-first approach to security

Software-based defences remain important, but threat actors now routinely pursue firmware and hardware-level weaknesses. Malicious code can be embedded deep within components, avoiding detection by conventional endpoint tools.

For enterprises running high-value on-prem workloads, this reinforces a fundamental truth: world class software requires equally robust hardware foundations. A hardware-first security model provides that assurance. Custom-engineered servers equipped with secure boot, hardware root of trust and tamper-resistant architecture ensure that only verified firmware and software can run.

Controlling the design, manufacturing route and supply chain of hardware reduces exposure to compromised components and supports alignment with strict governance and compliance requirements. For organisations handling sensitive or regulated data, this level of assurance is not optional.

## Operationalising threat detection and response

Security must function as an active, embedded discipline across the organisation. Real-time monitoring, behavioural analytics, and automated response capabilities now underpin effective defence.

Integrating Threat Detection and Response (TDR) directly into the server architecture delivers continuous visibility and rapid containment. This reduces pressure on internal teams, enhances overall system resilience, and preserves service availability.

An embedded approach enables a shift from reactive defence to proactive anticipation. Threat patterns can be identified sooner, risks assessed earlier and mitigations introduced before an incident takes hold. For organisations with business-critical software running on-prem, this proactive

posture is essential.

Network-level defence is equally important. Critical systems should sit behind strong firewalls and within segmented network zones. Only essential services should be exposed. Segmentation restricts lateral movement if a breach occurs. The NCSC advises designing architecture that protects internal systems from external threats and from one another.

## Designing for future adaptability

Technological change and regulatory evolution require infrastructure that is secure now and adaptable over time. Futureproofing involves careful planning for scalability, integration, and performance.

Bespoke on-prem server solutions allow organisations to tune infrastructure to the exact needs of their workloads while meeting industry standards and data protection requirements. Security must operate alongside speed and reliability. High-demand environments require both, and custom configuration supports this balance.

Adaptability also means preparing for new capabilities such as AI-driven analytics, edge computing and hybrid models that combine on-prem control with selective cloud flexibility. It includes anticipating changes to data sovereignty rules, cybersecurity frameworks, and sector-specific regulations.

When it comes to advanced analytics powered by AI, this will require servers capable of handling high-volume, low-latency data processing. Organisations will need hardware optimised for machine learning workloads, with secure accelerators and GPU integration to support predictive insights without exposing sensitive data. Edge computing deployments are also becoming essential for sectors where decision making is needed in real-time.

Building adaptability into hardware design reduces the complexity of future upgrades, maintains security posture, and ensures that advanced on-prem software continues to operate effectively as demands evolve.

## Infrastructure as a strategic asset

Server infrastructure has shifted from a passive IT component to a strategic asset that shapes organisational resilience. As threats become more advanced and regulatory pressures grow, UK organisations must adopt a comprehensive, forward-looking approach to server security.

By prioritising hardware-level protection, embedding intelligent threat detection and response and designing for long-term adaptability, enterprises can build on-prem infrastructure that is resilient, compliant, and aligned with their long-term goals.

When organisations invest in secure, fully customised servers that combine performance with strategic foresight, infrastructure becomes more than a defensive measure. It becomes a platform for delivering stronger outcomes to the customers, communities, and citizens they serve. ■

exacta  
technologies



## UNLEASH YOUR SOFTWARE

**Bespoke, fully branded servers, built to make your software shine.**

We design and build bespoke, fully branded servers that deliver fast, seamless performance for your customers. From manufacture to global logistics and support, we handle the hardware so you can focus on your software.

Discover custom hardware

[sales@exactatech.com](mailto:sales@exactatech.com) | [www.exactatech.com](http://www.exactatech.com)

## Independant UK Datacentres & Server Hosting

### Who we support:

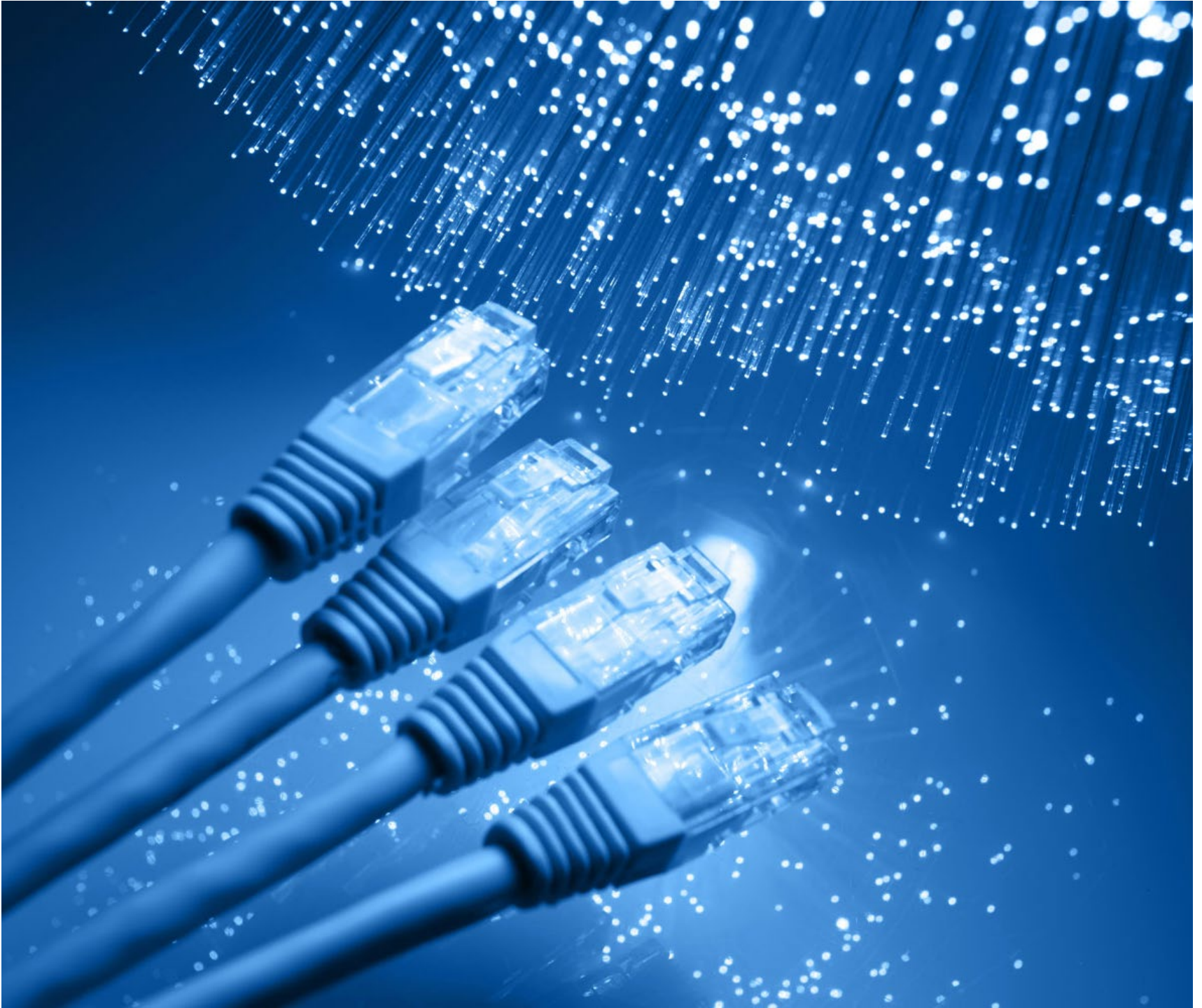
Clients ranging from  
**national & multinational companies to schools and small businesses.**



velox  
serv

**0800 084 3521**  
[www.veloxserv.co.uk](http://www.veloxserv.co.uk)





# SD-WAN isn't dead — it's relocating

**As UK enterprises grapple with hybrid work, rising cyber threats and an ever-expanding cloud footprint, the question keeps resurfacing: does SD-WAN still matter?**

## Hybrid work has changed the rules — but SD-WAN still holds the map

When hybrid work arrived, it didn't gently knock. It kicked the door off the hinges, scattered the network diagrams, and told IT teams to reinvent security before lunch. The old days of predictable branch offices and tidy perimeters are long gone; in their place is a muddier, more fragmented landscape where users,

apps and data live everywhere.

In this new reality, many predicted SD-WAN would fade away; but UK enterprise leaders argue the opposite.

"SD-WAN remains a foundational technology, providing the essential flexible and resilient connectivity every modern enterprise needs," says Anthony Senter, CEO & Co-Founder of ATOMNIA. "Businesses increasingly ask for SASE, but many don't realise that SASE simply combines secure access (SSE) with that same SD-WAN core. It's that unified combination that supports the hybrid workforce's demand for performance, security and reliability."

That misunderstanding reflects a shift in the market: SD-WAN hasn't disappeared, it has simply become the quiet partner in a larger solution.

Toby Sturridge, Senter's co-founder,

agrees, but adds that "SD-WAN's value absolutely endures, but moving forward, it must be delivered as a commodity, built in, not bolted on and never charged as a premium. The power lies in integrating SD-WAN seamlessly within a scalable solution, so enterprises stop paying extra for the connectivity foundation and instead invest in next-generation protection and management."

Mark Burski, Managing Director at Digital Carbon, says the pairing is not a competition but a co-dependency: "SD-WAN and SASE aren't competing. SD-WAN provides the optimised transport layer — broadband, 4G/5G, satellite — and the orchestration that makes hybrid work usable. SASE takes that foundation and adds the cloud-delivered security services: next-gen firewalls, CASB, secure web gateways, ZTNA. Together,

they create the unified edge architecture today's remote and distributed organisations need."

## The security wakeup call: SD-WAN alone can't fight today's threats

As UK enterprises opened up their networks to remote workers, cybercriminals opened up their wallets. With ransomware, phishing, credential theft and cloud attacks all surging, organisations have learned

Mark Burski,  
Digital Carbon

Leigh Walgate,  
Nasstar



the hard way that the perimeter now has more holes than a block of Swiss cheese.

“As the workforce becomes more dispersed and the attack surface expands, SD-WAN alone is not sufficient to address today’s cybersecurity challenges. Remote access, encrypted traffic, and cloud-based applications demand a zero-trust approach, deep traffic inspection, and unified policy enforcement. This is precisely where the SASE model comes in, providing a more comprehensive framework that integrates networking and security,” explains Eduardo Oliveira, CTO, MikroTik SD-WAN.

Indeed, SD-WAN strengthens the transport layer, but industry leaders are brutally honest about the limits of its defence.

Burski explains the divide: “SD-WAN delivers built-in firewalls, segmentation, encryption and IDS/IPS — excellent foundations for network-layer protection. But it’s not enough to defend against today’s complex, application-level threats. SASE adds advanced cloud-delivered capabilities — sandboxing, DLP, TLS inspection, threat intelligence — and applies them consistently no matter where users are working.”

It’s a security story IT teams know well: the tools we trusted for office-centric networks simply can’t cope with a world where the network is everywhere.

Leigh Walgate, Managing Director of Secure Networks at Nasstar, says the gap is often invisible until it becomes a headline: “SD-WAN focuses on protecting the boundaries of the corporate network and encrypting traffic over the internet. That’s valuable, but it doesn’t secure users, data or applications wherever they’re located. Modern threats don’t respect traditional perimeters. With cloud-hosted data and remote workers, people access applications directly over the internet, download files to personal devices and potentially expose corporate data through unmanaged channels.”

That’s why Zero Trust became more than a buzzword: it became a survival tactic.

“SASE enforces continuous verification of every user and every device, no matter where they are,” Walgate continues. “It delivers secure web filtering, CASB oversight, remote browser isolation and least-privilege access, so even if credentials are compromised, the attacker can’t move laterally. These are the vulnerabilities the NCSC warns UK businesses about, and they’re exactly the gaps SD-WAN alone cannot cover.”

Senter sees the industry shifting to a new mindset: “SD-WAN alone is no longer enough. The attack surface is expanding, and no single product provides comprehensive defence. SASE isn’t a security add-on, it’s a holistic framework that combines firewalling, CASB, ZTNA, SWG and data encryption into one cohesive model that protects remote teams wherever they are.”

The conclusion is clear: SD-WAN gets you connected; SASE keeps you protected.

## Cost, agility and a very British connectivity market

Unlike the US, where MPLS pricing can induce nausea, the UK market is more forgiving. That creates a unique situation: SD-WAN adoption here isn’t purely about slashing costs: it’s about

creating freedom.

Sturridge says the pricing debate is stuck in the past: “legacy views of SD-WAN as a premium alternative to MPLS are outdated. With solutions including SD-WAN as standard, organisations unlock real performance gains and often up to 50% cost savings compared with traditional MPLS, while reallocating budget to improve security. There’s no longer a trade-off between resilience, bandwidth and protection.”

But the biggest benefit isn’t pounds saved it’s hours saved, as Walgate explains: “in practice, the decision isn’t about MPLS versus the internet anymore. The internet is now the default for most requirements. The real savings come from simplified management and reduced licence sprawl when SD-WAN or SASE replace multiple point tools.”

And in a market with strong fibre competition, agile deployment matters more than ever.

“The business case for SD-WAN in the UK goes beyond headline reductions. The real value lies in agility: the ability to scale bandwidth, deploy new sites within minutes, support seasonal or project-based operations and avoid long-term circuit commitments. Even if the monthly savings are modest, the operational advantages are significant,” says Burski.

SD-WAN isn’t the cheapest tool in the box: but it’s often the smartest one.

## The future is hybrid: SD-WAN behind the scenes, SASE up front

If UK enterprises have learned anything, it’s that no single connectivity model wins the argument. MPLS still has its fans, SD-WAN still carries the load, and SASE is becoming the new north star for secure access.

The reality? Most organisations will use all three in some capacity.

“Modern hybrid policies demand more than a single solution,” says Senter. “The strongest approach is a fully converged, device-less SASE solution, bridging SD-

WAN, advanced security and next-gen access for offices and remote users alike. It removes the complexity and risk of legacy systems such as MPLS or VPN.”

“UK businesses should not view SD-WAN and SASE as competing technologies, but rather as complementary components of a hybrid approach. SD-WAN provides the intelligent connectivity backbone, while SASE layers on security and access controls for cloud and remote environments,” asserts Oliveira.

Walgate sees a pragmatic future: “many organisations will take a hybrid WAN approach, using SD-WAN and SSE alongside existing MPLS, then gradually reducing MPLS dependency as requirements evolve. There is no one-size-fits-all solution. What matters is aligning with the organisation’s digital transformation and Zero Trust journey.”

And Burski reinforces that hybrid isn’t temporary — it’s the blueprint: “for most UK organisations, the most effective approach is blended. Keep MPLS for workloads needing guaranteed performance, use SD-WAN overlays for agility, and extend secure access to remote workers via SASE gateways. Transformation usually starts with SD-WAN for visibility and optimisation, then SASE layers are added incrementally.”

In other words: the future network won’t pick sides: it will pick what works.

## SD-WAN isn’t fading. It’s evolving

What emerges from every expert is a rare consensus: SD-WAN isn’t disappearing. It’s simply becoming the connective tissue inside something bigger, in an industry shift that is already underway.

“The trend is clear: SD-WAN is becoming a built-in component within advanced solutions such as SASE. Providers offering only SD-WAN will struggle as markets prioritise agility, convenience and deep security all in one platform,” notes Senter.

Sturridge says the roadmap goes beyond consolidation: “expect sharper integration with AI-driven threat detection, quantum-ready encryption and customer-specific controls. The future is simplification and fully managed services — so networking and security never constrain innovation.”

“SD-WAN isn’t being replaced; it’s evolving as the intelligent transport layer within SASE. As architectures mature, organisations want fewer vendors, simplified operations and consistent user experiences. SD-WAN provides the application-aware routing and path selection that SASE still depends on,” adds Walgate.

Burski, meanwhile, sums up the long game: “SD-WAN’s role is shifting from standalone product to the performance engine underpinning SASE. As the UK expands fibre and 5G, SD-WAN remains vital for site connectivity and resilience, while SASE provides the cloud-delivered security required for hybrid work. The transition will be gradual, not a sudden replacement.”

## Is SD-WAN still relevant?

Absolutely — just not in the way it used to be. It’s no longer the headliner, because it has become the backbone. It’s the engine under SASE’s bonnet, powering the secure, hybrid, cloud-first networks UK enterprises depend on. ■



Anthony Senter, ATOMNIA



# Your Network. Your IT Team.

## Accelerated by Digital Carbon.

### Co-Managed SD-WAN Support, Training and Design — Without Losing Control.

- Faster Deployments, Deeper Visibility, Simpler Operations, Lower Costs
- SD-WAN Trials including 5G Fixed Wireless Access - No Obligations
- Arista VeloCloud SD-WAN - Secure, Cloud-ready, Carrier-agnostic
- Free SD-WAN Workshop for IT Teams - Book Now!

**DIGITAL CARBON**

**Visit For More**  **Click Here** [www.digitalcarbon.io](http://www.digitalcarbon.io)





## Optos Future-Proofs with Vodafone Business SD-WAN Partnership

- Optos is an innovative Scottish retinal imaging technology company that help to identify eye disease early and save thousands of people's sight across the globe.
- To continue expanding globally, Optos need robust and consistent connectivity to enable critical communication between teams.
- Vodafone Business SD-WAN gives Optos a consolidated, simplified connectivity solution that is easy to manage and consistent across every site.

Vodafone Business has signed a three-year agreement to deliver a Software-Defined Wide Area Network (SD-WAN) for Optos, an innovative Scottish retinal imaging technology company that help to identify eye disease early and save thousands of people's sight across the globe. Vodafone Business SD-WAN will help Optos consolidate disparate systems into a single network solution, ensuring optimised and robust connectivity globally.

**Vodafone Business SD-WAN** gives Optos real-time visibility and centralised control over their global network and allows them to manage and optimise the connectivity between sites more effectively, and keep systems simplified under a single network. With reliable and efficient information exchange now established between departments worldwide, connectivity issues are no longer a major concern, allowing Optos to allocate resources to innovation and business development.

Adam Shaw, Head of IT, Optos said: "Working with Vodafone Business has been transformative for Optos. Their SD-WAN solution gives us the secure, resilient connectivity we need to link our global sites and means we can grow our business without having to keep purchasing new technology – it grows with us. This collaboration ensures we can provide clinicians with the tools they need to continue their work to help protect vision for millions worldwide."

[Click for the full story below](#)

Connecting innovative  
eyecare technology



vodafone  
business







# Redefining the perimeter: observability and security in the age of cloud complexity

Pejman Tabassomi, Field CTO for EMEA, Datadog

**C**redential theft continues to pose a significant risk for enterprises operating in the cloud. In this environment, both human and machine identities now constitute the new security perimeter, meaning that a single leaked credential can provide attackers with access to an organisation's most sensitive data. This risk has prompted teams to rethink their security models and develop new strategies (such as data perimeters and multi-account governance) to reduce exposure while maintaining operational agility.

## The growing risk of credential theft

In cloud production environments, a crucial aspect of security involves automating repetitive tasks that are prone to human error when performed manually. Continuous integration and delivery (CI/CD) pipelines, for example, are responsible for deploying changes to infrastructure and applications. While these pipelines, often managed with Infrastructure as Code (IaC) tools or provider-specific scripts, help reduce human error, they also introduce potential vulnerabilities.

Credentials are a prime target for malicious actors as demonstrated by a massive data breach earlier this year, which exposed 16 billion login details. A common cause of data breaches in cloud environments is the misuse or leakage of long-lived credentials, as highlighted by our 2024 study. CI/CD pipelines typically run with elevated permissions, allowing leaked credentials to grant attackers extensive access to critical infrastructure.

The most effective way to mitigate these risks is to use short-lived access credentials that automatically expire after a short period. This limits the potential damage if they are compromised. However, our 2025 report shows that many organisations have not yet adopted this approach. For example, only about three in five companies using GitHub Actions rely exclusively on this more secure, "keyless" method of authentication. The rest still depend on older, long-lived access credentials that remain valid indefinitely, leaving them significantly more vulnerable if those keys are compromised.

Because APIs are exposed by design, attackers no longer need to infiltrate a network to compromise a system. Valid credentials alone are sufficient for access.

## New strategies

In response, organisations are adopting new strategies to protect their cloud environments beyond traditional network boundaries. One such approach is the use of data perimeters, which restrict access to cloud resources based on trusted networks, accounts, or organisational boundaries. According to the recent "State of Cloud Security" report, 40% of organisations have already established data perimeters (a notable achievement given the complexity involved). The most common implementation methods include S3 bucket policies, which limit access to approved AWS accounts, and VPC endpoint policies, which prevent unauthorised data exfiltration. A smaller number of organisations extend these boundaries at the organisational level to ensure that critical resources cannot be accessed from outside the enterprise.

Another emerging strategy is multi-account governance. Managing minimal

privileges within a single account can be challenging, leading many teams to use platforms like AWS Organisations to centrally manage multiple AWS accounts and enforce top-down security guardrails. This approach is gaining traction, with 86% of companies using multi-account structures, more than 70% of which include all accounts within the organisation.

Both strategies (data perimeters and multi-account governance) reflect a growing concern over credential theft and a willingness to adopt provider-supported guardrails to protect cloud data.

## Legacy credentials: an ongoing risk

Despite these advances, long-lived credentials continue to pose a significant threat. The report found that 59% of AWS IAM users, 55% of Google Cloud service accounts, and 40% of Microsoft Entra ID applications had access keys older than one year. Even more concerning, the proportion of keys older than three years has increased across multiple cloud providers, creating unmonitored access points that are rarely rotated and sometimes remain active in unused systems.

While 79% of organisations now use federated authentication for human users accessing the AWS console, through services like AWS IAM Identity Centre or Okta, almost two in five still depend on IAM users somewhere in their environments, with one in five using them exclusively. Many of these credentials are not only outdated but also unused. Over half of AWS IAM users with keys older than a year had not used them in the previous 90 days. This stagnation suggests that while organisations are starting to adopt modern practices, legacy credentials continue to be a persistent vulnerability.

## Observability as a security enabler

As the traditional network perimeter fades, observability has become a pillar of enterprise security. In an environment where attackers exploit valid credentials to blend in with regular activity, having visibility across systems, workloads, and identities is vital. Observability enables teams to detect vulnerabilities, validate controls, and respond to indications of compromise before issues escalate.

Unlike traditional monitoring, which typically focuses on collecting logs and metrics, observability creates a shared operational view. This allows engineering, operations, and security teams to correlate activities, trace events back to their sources, and understand behaviours across the entire environment. This capability is particularly valuable in addressing credential theft, as it highlights anomalies and links suspicious activities to known attacker tactics.

Observability also drives continuous improvement. By tracking detection efficiency, response times, and alert accuracy, organisations gain insights into the effectiveness of their defences. Additionally, it supports compliance by providing empirical evidence that security controls are functioning as intended, and it strengthens the defensive ecosystem by turning visibility from reactive firefighting to proactive investigations.



## Towards continuous, contextual security

In today's cloud environments, the security perimeter is no longer a fixed boundary. Every user and machine account represents a potential entry point to critical data. As attackers increasingly exploit stolen or compromised credentials, implementing robust access controls, using short-lived credentials, and ensuring continuous verification have become essential.

The path forward involves combining multiple strategies into a global, adaptive defence. Short-lived credentials, clearly defined data

perimeters, multi-account governance, and deep observability work together to provide contextual awareness across all interactions in the environment. Observability, in particular, enhances understanding of credential-based threats by connecting signals across users, systems, and networks, allowing teams to detect misuse early and take decisive action.

Security in the cloud era is no longer about building higher walls. It is about maintaining continuous, contextual awareness of every interaction, building defences in visibility and intelligent automation, reducing the impact of credential theft, and strengthening trust in systems and operational resilience. ■

READY TO STOP OVERPAYING  
FOR "JUST SD-WAN"?

OMNIA

Connection Protection Detection

- Fast, Resilient SD-WAN
- SASE, XDR, ZTNA
- Data Encryption
- Secure Remote Options
- Secure Cloud & IOT Access
- In-Country Gateways
- 24/7/365 Support
- Re-tech Promise



Advanced Affordable Scalable





# Why poor technology investments are undermining modern policing policy

Will Hitch, Public Safety Lead (UK & Ireland), Getac UK Ltd

**M**odern policing finds itself at a decisive point. On one hand, the depth and breadth of technology available has never been greater, but on the other, the challenges associated with effectively implementing it are at an all-time high.

Technology has always played a key role in policing. From the emergence of fingerprinting in the early 20th century, to the first successful use of DNA evidence in 1986, breakthroughs in technological innovation have often facilitated major leaps forward in police efficiency and crime reduction. Today, the use of CCTV, facial recognition, UAV and ANPR are commonplace, as forces up and down the UK increasingly look to harness technology to counteract resourcing challenges and an increasingly exacting policing landscape.

In particular, there's growing emphasis on promoting proficient 'Techcraft' amongst officers- which combines digital technology with traditional police fieldcraft to optimise results. However, while most officers are adept at using technology and are highly competent at their jobs, forces are struggling to combine the two together in the most effective way.

## Outdated technology is holding forces back

There are several reasons for this, chief among them being an over reliance on outdated technology infrastructure and field devices. Public sector funding is always a challenge and policing is no exception. But as a result, local level investment in new IT equipment has failed to keep pace with modern technology standards, to the point where officers out

mindsets like this only serve to exacerbate the ongoing problem.

## Overly ambitious tech projects struggle to reach completion

Another contributing factor to the technology issues facing many forces is the abundance of large-scale national tech projects that either experience significant delays or fail to reach completion. The scale of UK policing, particularly when it meshes with other areas of the UK security architecture, means many national-level projects – while necessary and important – are simply too ambitious from the start. A good example is the Emergency Services Network (ESN) project, which began in 2015 and was originally due for completion in 2019. However, after a series of major delays it is now not scheduled to be operational until 2029. While recent developments around the ESN give cause for optimism, with several companies teaming up to get the project back on track, these delays mean emergency services workers are currently still reliant on the outdated Airwave system over six years after the switchover was due to take place.

## Bringing people and technology together is crucial

In today's VUCA world, modern policing requires people and technology to work seamlessly together.

From a technology perspective, this starts with well-informed purchasing decisions made by technologically literate leaders, with the aim of meeting realistic timeframes and digital goals. In many cases, a great first step is investing in modern rugged

**"Technology has always played a key role in policing. From the emergence of fingerprinting in the early 20th century, to the first successful use of DNA evidence in 1986, breakthroughs in technological innovation have often facilitated major leaps forward in police efficiency and crime reduction."**

in the field can be using equipment that's significantly outdated compared to the technology they use in their personal lives.

In a recent study by Policing Insight, 55% of the 4,000 police officers questioned said they were not satisfied with their force's ICT provision, while just 50% said the information on their force's systems could be relied upon.

Stats like this paint a sobering picture for police services up and down the country. When officers lose faith in their equipment, not only do they become more reluctant to use it, but (with the best intentions) they can seek non-sanctioned alternatives, which puts sensitive evidence and data at risk in the process.

Further adding to this issue is a general reluctance amongst leadership teams – some of whom still see technology as a source of risk rather than opportunity – to commit the necessary levels of budget needed to bring front line equipment up to date. In many cases, this is due to fear of making an expensive mistake, but

laptops, tablets and ICT equipment that can be reliably used in the field without fear of damage or failure. Only by doing this can officers on the front lines begin to take advantage of the wealth of digital applications and services now available to them, from digital fingerprint recording and GPS mapping, to 3D crime scene rendering and AI-powered interview transcription.

From a people perspective, forces need to ensure everyone – from senior leadership to front line officers – receives the level of training needed to fully understand and capitalise on the opportunities that modern technology presents. This includes providing specialist training where required, particularly in rapidly growing areas such as data analytics, AI literacy and technical architecture. Empowering officers with these specialist skills will enable them to embrace new, technology-led methods and processes as soon as they become available, uplevelling the entire organisation in the process.

Police services up and down the UK increasingly need to harness the wealth of



powerful policing technology available to them in order to do their jobs effectively. However, a combination of underfunding/ investment at a local level, overly ambitious national projects, and reluctance from some senior leaders to embrace new digital solutions is making it very difficult for many

to achieve. Successful digital strategies must bring technology and people together in a way that ensures those tasked with adopting and using new technology fully understand its benefits and are confident using it from day one. Only then can truly data-driven policing become a reality. ■

## Protect Monitor Control

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

### How hot is your Server Room?

Contact us for a **FREE site survey** or **online demo** to learn more about our industry leading environmental monitoring solutions with **Ethernet and WiFi** connectivity, **over 20 sensor options** for temperature, humidity, water leakage, airflow, AC and DC power, a **5 year warranty** and automated email and SMS text alerts.

**Server Room environments** **0800 030 6838**  
[projects@serverroomenvironments.co.uk](mailto:projects@serverroomenvironments.co.uk)

Cooling
 Power
 Energy
 Fire
 Monitoring
 Racks
 Networking
 Consultancy
 Services



# Automation, sovereignty & cyber wars: what's next for 2026?

**Enterprise networking is heading into a year where automation grows up, cybersecurity gets more urgent, and digital sovereignty reshapes infrastructure choices across the UK...**

## How do you see AI-driven network automation reshaping IT operations?

John Smith, EMEA CTO, Veracode: In 2026, the biggest shift we'll see will be centred on automation finally becoming trustworthy enough to run itself. Like we've seen with the rise in vibe coding this year, AI-driven network tools will start taking over routine configuration and threat monitoring, which means IT and security teams will spend less time firefighting and more time validating what AI systems are doing.

Marcus Bentley, ICT Solutions Architect, Kyocera Document Solutions UK: The shift from manual network administration to policy-driven automation is accelerating. We're seeing organisations leveraging data analytics for capacity planning and automated fault remediation, with AI recommendations set to play a major role in future network development. As automation advances, traditional configuration skills will inevitably decline, giving rise to new roles such as AIOps specialists and engineers focused on policy-based management and AI scripting.

Greg Jones, Senior Vice President of MSP Enablement (EMEA & North America), Kaseya: AI is still in its early stages, and its potential is extraordinary. We have only just begun to see how it can transform operations, drive efficiency and unlock entirely new ways to deliver outcomes that matter. We are also seeing the rise of data-driven MSPs that use analytics, automation and AI insights to make smarter business decisions, predict client needs and measure outcomes in real time. Rather than reacting to issues, these MSPs operate proactively, anticipating challenges before they arise and proving value through measurable business impact.

## With the UK pushing for digital sovereignty, how will local regulations influence network architecture?

Aaron Allsbrook, CTO, ClearBlade: We're seeing a proliferation of data centres, meaning the cloud will be more distributed with more locations. As this happens,

networks will become distributed data centres that automatically enforce regional regulations (like GDPR's Model Clauses), much in the way current tools implement tax codes. This will simplify compliance for enterprises as networks will know which setups to honour in a more localised and automated fashion.

Álvaro Gómez, Senior Network Consultant, Kocho: Local regulations will accelerate hybrid and multi-cloud strategies, with enterprises prioritising UK-based data centres to store and process their data for compliance purposes. Network architectures will need to incorporate compliance-aware data location, routing of data and encryption, ensuring data residency and regulatory adherence without compromising performance. The biggest challenge will be securing and managing distributed edge nodes at scale. Enterprises will need robust orchestration tools and AI-driven monitoring to maintain visibility and enforce consistent policies across fragmented environments.

Smith: New UK data sovereignty rules will push companies towards more localised, hybrid architectures, and increasing complexity in the supply chain just as automation scales up. With GenAI models choosing insecure code 45% of the time, the challenge will be keeping automated networks secure and accountable, not just building smarter new ones.

Scott Gray, Product Marketing Manager, 11:11 Systems: Enterprises will fully standardise hybrid and multi-cloud architectures to optimise cost, cyber resilience, and compliance. Network-as-a-Service (NaaS) will emerge as a critical enabler, offering the on-demand, software-defined connectivity needed to manage distributed environments. Expect centralised policies, usage-based pricing, and simpler integration across data centres, clouds, and edge sites.

## What are your expectations for cybersecurity strategies for UK enterprises in 2026?

Mike Puglia, Kaseya Labs General Manager: Up until now, law enforcement and governments have been making rules for organisations to protect themselves, which is only one part of the solution.

With recent arrests in the US and Europe of cyber-attackers, we are starting to see them 'join the fight' as they do with any other type of crime.

Gray: Organisations will deepen their commitment to cyber resilience by maturing their zero trust security models. The increasing use of AI in cybersecurity tools will drive a focus on continuous verification, identity-first controls, and a significant reduction of the attack surface. Pervasive multifactor authentication (MFA), passwordless solutions, and micro-segmentation will become standard practice. AI-powered automation and threat intelligence will be instrumental in enhancing detection and response capabilities, drastically reducing threat dwell times and allowing teams to neutralise attacks faster.

**"AI is set to become the most transformative force in networking. By automating threat detection, predicting performance issues, and guiding scalable network design, AI enables faster, smarter decisions."**

Micah Deriso, Global Head of Channel at Verkada: As security technologies become more integrated and valuable across organisations, we expect more decision-makers will be involved in the buying process – including groups like IT, HR, and operations. Organisations will need partners who understand how security fits into these broader business ecosystems and can communicate how modern security solutions can facilitate smoother operations, improve visitor management, and provide actionable data insights.

Babak Behzad, Head of AI at Verkada: Agentic AI tools will be able to power a security operator's entire workflow, enabling them to focus on their highest-value work: AI is already redefining what it means to secure the physical world. Tools to date have been focused primarily on speeding up investigations, and while that is incredibly valuable, it's really just the start of what AI can do. As AI models become more capable and intuitive, they'll transform physical security into a proactive, intelligent discipline that helps teams detect and deter incidents before they escalate, not just respond after the fact.

## If you had to bet a pint on one major disruption to the UK enterprise networking market, what would it be?

Gómez: Quantum computing breaking actual encryption protocols, forcing the need to update protocols and technologies, to the ones that are resistant to quantum computing, and making obsolete most of the encryption protocols used today to protect traffic over the internet.

Puglia: Every single company is under enormous pressure to 'deploy AI' – it's the wild west as organisations bring the technology in-house to replace processes, customer-interaction, etc., which will perhaps be the largest deployment of an

untested/poorly understood technology in IT history. We simply don't have IT teams with technical experience in AI and there is virtually zero understanding of what/how to monitor from a cybersecurity perspective.

Allsbrook: AI and widely used common standards allow for small changes to have huge impacts. This is highly likely to result in a major physical disruption, whether through error or attack, much like we saw this year with major outages from small issues at cloud providers. These disruptions create a major loss of trust between enterprises and their network providers; we may see less reliance on major network providers as a result.

Bentley: AI is set to become the most transformative force in networking. By automating threat detection, predicting performance issues, and guiding scalable network design, AI enables faster, smarter decisions. It could even recommend when private 5G is preferable to wireless LAN, optimising for capacity, latency, and security. I firmly believe this shift will drive consistent, automated deployment across entire network estates, making cloud computing, edge computing, and end-user mobility more secure and efficient than traditional manual approaches ever could. ■



Marcus Bentley, Kyocera Document Solutions UK

John Smith, Veracode

Aaron Allsbrook, ClearBlade

Mike Puglia, Kaseya

Álvaro Gómez, Kocho





# Strengthening patient care with a future-ready network

**W**irral University Teaching Hospital (WUTH), one of the NHS's leading digital trusts, has transformed its ability to deliver responsive, high-quality patient care thanks to a major core-to-edge network upgrade delivered by HPE Pointnext, Aruba and long-term partner Stoneleigh Consultancy Ltd. For a trust where clinicians rely on instant access to electronic records, PACS images and mobile apps at the bedside, the old infrastructure had become a bottleneck that was increasingly hard to ignore.

The problem was straightforward, and painful. As the hospital rolled out new digital services, the legacy wired network struggled to keep up, causing outages, limitations on new applications, and rising support costs. Wireless performance had already improved following WUTH's move to Aruba, but the wired estate remained a weak link.

"We wanted to use our Cerner Millennium system to support mobile devices at the patient's bedside," recalls Phil Scott, Delivery Manager Head of Informatics at WUTH. "But our network was preventing us from realising the level of service our patients demanded."

Created in 1992, the trust depends on reliable connectivity across multiple sites to ensure clinicians can access crucial medical information when it matters most. If the network falters, so does the quality of care. With outages becoming more frequent, it was clear the time had come to build something far more resilient, scalable and ready for the future.

## A partnership built on trust

WUTH didn't just want new hardware. They wanted a partnership. After dealing

with the complexity of juggling multiple vendors and mismatched technologies, the trust sought a single, integrated solution — one that could be deployed with zero disruption and provide a strong foundation for long-term innovation.

Aruba and HPE Pointnext teamed up with Stoneleigh Consultancy Ltd., a longstanding local systems integrator with deep healthcare expertise and intimate knowledge of WUTH's environment. Stoneleigh had previously implemented WUTH's network, giving them rare insight into the trust's operational realities.

"In choosing a new vendor for the network upgrade, we were looking for more than a technology solution," says Scott. "We wanted one partner to advise on the design, ensure a seamless migration, support operations and transfer knowledge to our team."

HPE Pointnext's track record of delivering critical infrastructure projects proved decisive. Their consultants brought proven methodologies developed across countless similar engagements, collaborating closely with Stoneleigh to design a network that would be simpler, more resilient and capable of absorbing future demands.

## Designing for zero downtime

Reliability was paramount. The new design centred on resilience, availability and ease of management, using HPE Intelligent Resilient Framework (IRF) technology for built-in failover and full utilisation of network bandwidth. The solution employed HPE FlexFabric 5900AF switches at the core and HPE FlexNetwork 5130 PoE+ switches at the edge, ensuring

a consistent, high-performing experience for users across the trust.

To support WUTH's heavy reliance on PACS and other high-bandwidth services, the architecture incorporated 20 GbE switch uplinks and 80 GbE of core bandwidth. Redundant power, LACP active/active uplinks and resilient L2/L3 protocols eliminated common points of failure. Meanwhile, HPE Intelligent Management Center and Network Traffic Analyser software gave IT a single, unified view of the entire network.

Security was woven throughout, with SSH, TACACS and HPE IMC TACACS+ Authentication Manager strengthening access control and accountability. The design also ensured seamless support for Wi-Fi, IP telephony and QoS-sensitive services.

When deployment began, the goal was simple: no disruption.

"Some staff contacted me to ask when the deployment was happening," says Scott. "I was thrilled to tell them it had already been completed and they hadn't even noticed. That's the kind of value HPE Pointnext and Stoneleigh brought."

## A network that just works

The impact was immediate. Network instability, and the complaints that came with it, vanished almost overnight. Clinicians using more than 700 iPads to access patient information across wards no longer experienced dropouts or black spots.

"Wi-Fi is like electricity," says Scott. "You only hear about it if it's not working. And we've stopped hearing about it altogether."

To keep the new infrastructure running

at its best, the trust adopted HPE Proactive Care for its core switches and HPE Foundation Care across the edge. This combination gives WUTH predictive insights, faster issue resolution and access to HPE specialists whenever deeper expertise is required. As Scott puts it, HPE Pointnext has become "an extension of our team," supporting day-to-day operations while providing backup for more complex challenges.

Knowledge transfer has been a critical part of the partnership. HPE Pointnext ensured WUTH's IT staff gained both the tools and the confidence to manage the environment independently, with expert support only ever a phone call away.

## Building a digital future

For WUTH, the upgrade is more than a technical milestone — it's a platform for continued digital innovation. The trust can now deploy new applications at speed, deliver consistently high-quality connectivity across hospital sites and ensure clinicians always have the information they need at the point of care.

It's also helped cement WUTH's status as one of the NHS's leading digital organisations. The trust has been recognised as a global digital centre of excellence, offering it the chance to help other hospitals worldwide accelerate their own digital journeys.

"The success of the installation hasn't just solved today's problems," says Scott. "It's enabled us to keep innovating and ensure the best possible healthcare for our patients. Our business is to make patients better. Thanks to HPE and Stoneleigh, we now have a network we can rely on and the capacity to keep moving forward." ■





# The next risk for tech leaders: a shrinking talent pipeline

Imran Akhtar, Head of Academy, mthree

**A**rtificial intelligence is transforming how technology teams work. Tasks that once took hours now take minutes. As teams grow leaner, many employers are cutting back on graduate and entry-level hiring, assuming that having smarter tools means requiring fewer hands.

The reality? This short-term logic risks creating a long-term gap in skills and, more importantly, experience that could stall an organisation's progress for years.

Across banking, the public sector and large technology firms, work is evolving. While AI can help teams to deliver results more quickly, businesses still need reliable people who understand systems and keep services running during complex scenarios. When organisations cut back on entry-level roles, they may save costs in the short term, but they also weaken the flow of future talent that keeps operations strong in the long term.

## The new shape of tech talent

As AI takes on more of the routine work involved in building and running systems, technical skills remain essential. They're still the foundation, but they're no longer the full picture. Employers now place greater importance on how people think, communicate and solve problems. Valuing those who can ask the right questions and explain ideas clearly to colleagues who aren't specialists is key.

**"Across banking, the public sector and large technology firms, work is evolving. While AI can help teams to deliver results more quickly, businesses still need reliable people who understand systems and keep services running during complex scenarios."**

This shift has changed what a strong early-career hire looks like. Curiosity and adaptability now sit alongside technical ability when employers assess potential. People who combine these qualities are better equipped to use AI responsibly - not just to speed up delivery, but also to apply sound judgment when reviewing its results.

## When efficiency becomes fragility

Scaling back early-career hiring can seem like an efficient choice. However, smaller teams delivering more often lead to greater risk over time. Senior staff end up managing day-to-day operations instead of focusing on innovation, and fewer new professionals gain the exposure they need to learn core systems and business processes. Knowledge starts to concentrate in a few experienced people, and when they move on, it takes months - even years - for replacements to reach the same level of understanding.

This imbalance doesn't only affect output; it also impacts culture. Without a mix of experience and energy, teams can lose momentum and creativity. A workforce that looks efficient on paper can quickly become stretched, with senior employees covering gaps that should belong to the next generation.

## Building capability for the long

### term

The solution lies in developing structured pathways that prepare individuals for real work before they join a real team. Models such as 'Hire Train Deploy' bring recruitment and training together, selecting candidates for potential and mindset as much as for technical ability. They receive focused preparation in the areas employers need most, so they can make an impact from day one.

This collective approach to learning helps new hires settle more quickly, reach consistent standards, all the while freeing senior staff to concentrate on higher-value work. Expanding entry routes through apprenticeships and non-degree options also widens access to motivated people who might otherwise be overlooked, creating a more diverse and loyal workforce - a real win-win.

Once employees are in role, professional development should continue with a clear structure and support. Giving early-career professionals the chance to rotate through different divisions within a technology organisation helps them see how their work connects to wider goals. Regular feedback, practical coaching and involvement in live projects allow them to build confidence and judgment through learned experience. Over time, these habits create individuals who take ownership of outcomes, not just to work on pre-assigned tasks.

## Measuring resilience, not just speed

As AI accelerates delivery, organisations need to ensure that progress remains sustainable. Measuring only how quickly work is completed gives an incomplete view of performance. True resilience lies in how well teams respond when things go wrong, including how quickly they can resolve issues, adapt to change and maintain performance when key people are unavailable.

Indicators such as issue-resolution times, staff retention and coverage for critical roles show whether that resilience is in place. When those measures begin to slip, it often means experience has become too concentrated at the top and that short-term efficiency is being achieved at the expense of long-term strength.

External partners can also help build resilience when they're used to strengthen internal capability rather than to replace it. The most rewarding collaborations align training with the organisation's own culture, systems and expectations - ensuring knowledge stays in-house while new talent arrives ready to contribute.

## Preparing people and technology together

AI should be seen as an amplifier of human capability, not a replacement for it. The organisations that will lead are those that



combine efficient teams with a steady flow of early-career talent who understand both technology and its wider purpose. Maintaining balance between junior and senior roles and embedding AI awareness across every team helps to build a workforce that is adaptable, capable and resilient.

By continuing to invest in junior talent, businesses can move faster without losing stability, ensuring that innovation remains

sustainable rather than short-lived. AI may accelerate delivery, but people sustain it - and that's what keeps progress moving in a positive direction. ■

CableFree  
**5G**  
Networks

## CableFree Complete 5G Network Solutions:

5G Small Cells

5G Core/EPC

Private SIM cards

5G CPEs

Optional NMS & Billing

Build your own Private 5G Network today:

UK Design & Manufacture

[www.cablefree.net](http://www.cablefree.net)





# Navigating in-building connectivity options

Stephen Patrick, CEO/founder, CableFree: Wireless Excellence

With the rollout of 5G accelerating across the country, IT teams face the challenge of ensuring seamless indoor coverage where outdoor signals often falter due to building materials like concrete and glass. Poor connectivity can lead to productivity losses, frustrated employees, and missed opportunities in sectors like healthcare, retail, and finance.

## Understanding the options

UK IT teams have several pathways to enhance indoor wireless coverage, but the choice depends on factors like building size, user density, budget, and future-proofing needs.

1. **Wi-Fi networks:** Often the first line of defense, Wi-Fi leverages existing internet connections to provide indoor access. It's cost-effective for data-heavy applications and easy to deploy using access points. However, Wi-Fi struggles with voice calls, high latency in crowded environments, and security vulnerabilities. In the UK, Wi-Fi 6 and upcoming Wi-Fi 7 offer improvements in speed and efficiency, but they don't inherently support cellular services like 4G or 5G handover.
2. **Distributed Antenna Systems (DAS):** DAS amplifies outdoor cellular signals through a network of antennas distributed throughout a building. Active DAS uses fibre optics for high-capacity distribution, while passive DAS relies on coaxial cables. Ideal for large venues like stadiums or

hospitals, DAS supports multiple carriers (neutral host capability) and integrates well with 5G. However, it's expensive to install — often 75% more than alternatives — and requires carrier approvals, which can delay rollout in the UK. For buildings needing robust 5G coverage, 5G DAS is crucial, as it addresses signal penetration issues in urban areas.

3. **Small cells:** These compact base stations extend 4G and 5G networks indoors, acting as mini cell towers. Unlike DAS, small cells can be carrier-specific or multi-operator, offering targeted capacity boosts. They're scalable, easier to deploy in smaller spaces, and support private networks, which are gaining traction in the UK for industries like manufacturing. Small cells are seen as the future of in-building connectivity due to their flexibility and lower costs compared to DAS.

Other options include off-air repeaters, which boost external signals without backhaul, and neutral host networks that allow shared infrastructure among operators. IT teams should assess building-specific needs: for example, Wi-Fi suits low-density offices, while DAS or small cells are better for high-traffic environments.

## What to look for in a small cell

As 5G adoption surges, small cells emerge as a versatile choice for UK IT teams. Here's what to prioritise:

- **Coverage and capacity:** Ensure the

solution delivers uniform signal strength across floors and zones. Look for multi-band support (e.g., sub-6 GHz for 5G) to handle varying user loads. Advanced features like beamforming and MIMO (Multiple Input Multiple Output) enhance performance in dense areas.

- **Scalability and flexibility:** Opt for modular designs that allow easy expansion as needs grow. Software-defined radios (SDRs) enable over-the-air updates, reducing hardware swaps. For UK compliance, confirm adherence to Ofcom's spectrum rules and ETSI standards.
- **Integration and deployment:** Seamless integration with core networks (EPC for 4G, 5GC for 5G) is vital. Plug-and-play options minimise downtime, while backhaul compatibility (e.g., fibre or microwave) ensures reliable connectivity. Consider power efficiency to align with UK's net-zero goals.
- **Security and management:** Features like encryption, firewalls, and remote monitoring protect against threats. Analytics tools for traffic optimisation add value.
- **Cost-effectiveness:** Balance upfront costs with long-term savings. Small cells often cost less than DAS, with ROI through improved productivity.

## Selecting a vendor

Choosing a vendor is as critical as the technology itself. UK IT teams should evaluate:

- **Reputation and track record:** Seek vendors with proven UK installations.
- **Support and services:** Prioritise 24/7 technical support, training, and maintenance. Vendors offering end-to-end solutions — from planning to optimisation — reduce complexity.
- **Compliance and innovation:** Ensure alignment with UK regulations, including data protection (GDPR) and environmental standards. Look for R&D investment in 6G readiness.
- **Case studies and partnerships:** Review testimonials and operator collaborations. Cost transparency, including TCO (Total Cost of Ownership), helps in budgeting.
- **Sustainability:** With the UK's green agenda, choose vendors using energy-efficient tech.

By weighing these, IT teams can avoid vendor lock-in and ensure long-term viability.

## Conclusion

For UK IT teams, selecting in-building connectivity involves balancing immediate needs with future demands. While Wi-Fi and DAS remain viable, small cells offer a forward-looking path for 4G and 5G. By focusing on coverage, scalability, and vendor reliability, teams can foster connected environments that drive innovation. As 5G evolves, proactive evaluation will keep businesses competitive in a wireless world. ■

## PRODUCTS

■ The **Amphenol Procom UWB-I 380-6000** is an ultra-wideband omnidirectional antenna designed for indoor Distributed Antenna Systems (DAS).

Supporting a broad frequency range from 380MHz to 6000MHz, it is suitable for multiple wireless technologies, including TETRA, GSM, DCS, PCS, UMTS, Wi-Fi (2.4 and 5.6 GHz), 4G LTE, and WiMax. The antenna features a low-profile, multiband design that is ground-plane independent, allowing versatile installation options both above and below ceilings without the need for an external ground plane. It comes with an external coaxial cable equipped with an N-female connector for easy setup.

The antenna provides omnidirectional coverage, ensuring consistent signal distribution in all directions, and operates with a maximum input power of 50W. Its polarisation is vertical, impedance is 50Ω, and it boasts a gain of -2.2dBd (0dBi). The antenna's VSWR is maintained below 2.0:1, ensuring efficient signal transmission. With passive intermodulation levels below -140 dBc, the UWB-I 380-6000 is a reliable solution for comprehensive indoor RF coverage across multiple frequency bands.



■ The **BTI WIRELESS CPX60P** is an advanced indoor 5G Sub-6 GHz CPE designed to deliver high-speed, reliable wireless connectivity for residential and business environments.

Powered by the Qualcomm SDX62 chipset, it supports dual-mode 5G NR and LTE-A CAT20, ensuring compatibility across a broad range of spectrum bands including N1, N2, N3, and more. Supporting both stand-alone (SA) and non-standalone (NSA) architectures, it offers flexible deployment options. The device is equipped with Wi-Fi 6 (802.11ax), providing fast wireless speeds, and features two gigabit Ethernet ports plus an optional voice POTS port for versatile connectivity.

Its eight cellular antennas and two Wi-Fi antennas ensure strong signal reception and coverage. Compactly designed at 105 mm x 105 mm x 215 mm and weighing under 1 kg, the CPX60P supports web-based, TR069, and SNMP management for easy remote configuration. Security

features include firewalls and filtering for MAC, IP, and URLs, safeguarding user data. With external power supply, this device eliminates the need for underground or aerial cabling, offering a seamless, cable-free broadband experience suitable for various indoor applications.



■ The **Boost Pro DAS SME Smart Signal Booster** is a carrier-grade solution designed to enhance cellular voice and data coverage in small and medium premises such as offices, banks, pubs and clubs.

Capable of covering up to 1,500 m<sup>2</sup> (15,000 ft<sup>2</sup>) with a system gain of 100dB, it ensures robust indoor connectivity. Built for bands 1, 3, 7, 8, and 20, the device features an intuitive setup process and a sleek, attractive design suitable for various environments. Its advanced IntelliBoost chipset, a six-core baseband processor, optimises indoor transmission and reception of 3G, 4G, and LTE signals through sophisticated filtering,

equalisation, and echo cancellation techniques, delivering superior data rates and consistent connectivity.

The system includes donor and server antennas, with options to expand using outdoor or multiple server antennas. It employs self-organising edge intelligence and automatic gain control to prevent interference with other wireless devices, ensuring network safety and high performance. Operating within a temperature range of 0°C to 40°C and humidity levels up to 95%, it measures 163mm x 158mm x 80mm and offers reliable, high-quality cellular coverage, making it suitable for various indoor environments.

■ The **Vicinity 5G Indoor Small Cell**, model Bristol5G-010, is a compact, all-in-one solution built on the Qualcomm FSM100 5G RAN platform.

Designed to enhance indoor network coverage, it addresses common challenges such as weak signals, blind spots, and interference, significantly improving connectivity and user experience within enclosed spaces. The device features an integrated small cell design that is easy to deploy and consumes low power, making it suitable for various indoor environments. Supporting 3GPP Release 15 standards, it operates in the N78 frequency band (3300-3800MHz) with bandwidth options of 40, 60, 80, or 100MHz. It supports multi-mode synchronisation through GPS or IEEE1588V2 (optional) and employs TDD duplexing with 256 QAM and 64 QAM modulation for downlink and uplink respectively.

With a maximum output power of 24dBm and support for up to 64 active users per cell, it ensures robust capacity and performance. The small cell includes system management and monitoring software for easy deployment, with dimensions of 240mm x 63.5mm x 240mm, weighing under 2.9kg, and operating efficiently at temperatures between -10°C to +40°C. Its IP31 rating guarantees protection against dust and water ingress.







# Please meet...

**Matthew Thompson, Managing Director – Europe, Airsys**

## Which law would you most like to change?

I would ban the sale of chewing gum. A persistent source of annoyance and irritation of mine is chewing gum and people's inability to discard it into a rubbish bin, and instead spit it onto the pavement. The discarded chewing gum then lies in wait ready for an unsuspecting pedestrian to step on it and in my experience usually when you are wearing your favourite shoes or trainers. Additionally, discarded chewing gum creates unsightly pavements and footpaths, and I have no doubt is difficult and expensive for local councils and businesses to remove. For the preservation of good footwear and pristine pavements, I advocate the ban of selling chewing gum.

## Where would you live if money was no object?

In the words of Dorothy from the Wizard of Oz, there is no place like home. I would probably still live in the UK and have a fondness for Devon, the Isle of Wight and the Yorkshire Dales & Moors, but still undecided on exactly where I would live in the UK. In my opinion, nothing beats a beautiful summer's day in the countryside in the UK.

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

As child, due to my fascination with Indiana Jones, it was to become a renowned archaeologist. That's until I realised it wasn't all high adventure and globetrotting. To be honest, I loved history at school, that is until I started GCSE history. It wasn't so much about the WWII, Viking invasions and the Roman Empire, but more Victorian poor laws and workhouses. That's how to kill a child's ambitions.

However, as a child I was also fascinated with design and engineering, which ultimately led me into mechanical engineering and where I am today.

## Who was your hero when you were growing up?

If this question allows for fictional heroes, then it would have to be renowned archaeologist Dr Henry Jones Jr AKA Indiana Jones. Growing up in the 80's, I loved the high adventure and action of the Indiana Jones movies. I wanted to be Indy! He had the brains, the brawn and mostly won the heart of the love interest. However, he was relatable. He was fallible, as most of us are. He made mistakes, had fears (snakes in the case of Indy) and got bruised, exhausted, and fed up. But no matter how beat he was, Indy always got back to his feet and took on the challenge head on with a dry, sarcastic wit. I admired that and still do to this day. Indiana Jones is the ultimate lovable rogue.

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

That is a real tricky one. You'll be thinking Harrison Ford, because of my love of Indiana Jones. But in truth, I would probably choose Alexander the Great. Educated by Aristotle, Alexander conquered much of the known world in just over a decade. He would have countless stories about his military campaigns and travels across Greece, Egypt and Persia.

## What was your big career break?

Working for Airsys: I started working for Airsys in early 2018 and was promoted to

Operations Director and then Managing Director towards the end of 2019. It was a great career move.

Airsys remains a privately owned business, led by its founder Yunshui Chen — a visionary and inspiring leader who is genuinely passionate about innovation. I believe Yunshui saw potential in me, and I'm sincerely grateful for the trust he placed in me to lead the European team.

My time with Airsys has allowed me to grow not only as a business leader but also as an individual. It's an experience that has shaped who I am today, and one for which I am truly thankful.

## What's the greatest technological advancement in your lifetime?

It pains me to say it, but probably Tim Berners Lee inventing the World Wide Web in 1989. Although I have reservations about the internet, it is ultimately a force for good, connecting the world, providing instant access to information (and sadly fake information), enhances communication, allowing for online shopping, learning resources, banking and entertainment to name just a few.

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

"Don't judge everyone by your own standards, you'll only disappoint yourself." Once you accept this, both your work and your personal life become easier to navigate.

## The Rolling Stones or the Beatles?

A real tough one. Both have a fantastic back catalogue, but as the Airsys UK HQ is in the northwest and I work with numerous Liverpudlians, for a quieter life I best say the Beatles. ■

# 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](http://www.MobileMark.com)

Contact Us Now:

+44 1543 459555

[enquiries@MobileMarkEurope.co.uk](mailto:enquiries@MobileMarkEurope.co.uk)

