NETWORKING+

Risky business?
Storms surrounding the public cloud
Mark Lewis, Pulsant, p5

Critical issues
Building trust in AI SOC analyst solutions
Brett Candon, Dropzone AI, p6

AI infrastructure investment
What major investments mean for the future of tech
Amritesh Anand, In2IT Technologies, p7

Network overload risk from rise of agentic AI

A new report from InterDigital, Inc., the wireless, video and AI technology research and development company, and market research firm ABI Research explores how the emergence of agentic AI will redefine the demands placed on devices, networks and cloud infrastructure.

The report, titled 'The Distributed Network Shift Enabling AI on Device', finds that the rapid adoption of agentic systems is expected to increase across enterprise and consumer markets over the next three years. Unlike traditional mobile applications that primarily consume data via downlink, agentic AI systems continuously generate and exchange contextual information to enable real-time reasoning and decision making.

Modern mobile networks have historically been optimised for downlink throughput and video delivery. However, as AI devices generate increasing volumes of upstream data, networks risk becoming overloaded, leading to higher latency and costs. The main devices driving uplink traffic include:

- Smart glasses, which continuously capture video, images and environmental context, sending data upstream for real-time AI inference and assistance. ABI Research predicts 70 million smart glasses shipments by 2030, with cellular-enabled devices representing more than 12% of shipments.
- Wearables, including next-generation wearables that collect voice, biometric and contextual signals to support persistent agentic AI interactions.
- Smartphones, which increasingly transmit multimodal inputs such as voice, photos, video and sensor data to cloud and edge AI systems.
- IoT sensors and devices, which continuously stream operational or environmental data to AI models for analysis, automation, and decision-making.

Uplink pressures are already visible in video-heavy applications such as livestreaming and real-time video collaboration, where many users uploading simultaneously can create localized cell congestion. Unlike these temporary spikes, agentic AI systems will generate continuous upstream data exchanges from connected devices, potentially creating sustained pressure on uplink capacity.

The report finds that to meet AI demands of modern devices, the industry must transition toward distributed intelligence architectures, where AI workloads are orchestrated across on-device processors, and cloud platforms based on their complexity. It argues that embedding intelligence deeper into network infrastructure will ensure AI-enabled applications can operate efficiently without compromising on performance.

"Agentic AI marks the next phase in the evolution of intelligent connectivity," said Rajesh Pankaj, chief technology officer, InterDigital. "As AI systems become capable of reasoning, planning and executing tasks autonomously, we are beginning to re-imagine our wireless networks for 6G. Intelligence must be distributed across devices, networks and the cloud, and delivering these AI-enhanced services efficiently will require a new computing architecture that balances performance, latency and energy efficiency."

"Agentic AI introduces a new set of requirements for both networks and devices," said Larbi Belkhit, and Paul Schell, senior analysts at ABI Research and co-authors of the report. "Supporting autonomous AI systems will demand far more distributed computing architectures and significantly more intelligent networks. Operators will need to manage increasingly symmetrical traffic patterns while enabling real-time AI workloads across device, edge, and cloud."

InterDigital is a global research and development company focused primarily on wireless, video, AI and related technologies. It designs and develops foundational technologies that enable connected, immersive experiences in a broad range of communications and entertainment products and services. ■

IN DEPTH: Infrastructure p7-8

New digital 'V-levels' introduced to help bridge the UK's AI skills gap

The UK government has introduced a new digital V-level qualification designed to help tackle the country's growing AI and digital skills shortage while simplifying England's complex post-16 education system.

Launching from 2027, 'digital' will be one of the first subjects available under the new V-level qualification, alongside education and early years and finance and accounting. V-levels will sit between A-levels and T-levels as a third Level 3 route, allowing students to combine vocational learning with traditional academic subjects.

The reforms aim to streamline the current mix of qualifications – which includes A-levels, T-levels, BTECs and other technical courses – into three clearer pathways, which are A-levels (academic), T-levels (technical), and V-levels (vocational).

Ministers say the digital V-level will give students a flexible way to build practical digital and AI-related skills without committing to a highly specialised technical pathway at age 16. Education Secretary Bridget Phillipson said the reforms are also intended to challenge the perceived hierarchy between academic and vocational routes and support the government's ambition to ensure two-thirds of young people are in education, training or apprenticeships by age 25.

The qualification is being introduced as businesses warn that AI adoption is outpacing workforce skills. While the UK is currently the third-largest AI market globally, industry leaders say the country risks falling behind without urgent investment in digital capability.

Each V-level will be equivalent in size to one A-level, enabling students to combine digital studies with subjects such as maths, economics or English, creating a more flexible pathway into university or the workforce. The wider reform programme will roll out gradually, with full implementation planned by 2030, while colleges and training providers prepare transition plans over the next four years.

Sheila Flavell, CBE, COO, FDM Group commented: "The introduction of digital V-levels as an important step toward closing the UK's AI skills gap. Graduates are entering a job market where entry-level roles are shrinking, yet AI and digital capabilities are becoming essential for nearly every role. Flexible vocational qualifications like digital V-levels give students the opportunity to gain practical, industry-relevant skills alongside academic study, helping them become job-ready and future-ready.

However, qualifications alone aren't enough. Employers, government, and education providers must work together to build strong early-career pipelines, offering hands-on experience and structured training. Only then can the UK develop a workforce capable of navigating the next decade of AI-driven transformation." ■

O2 and Ontix deploy small cells to boost capacity in Bath

O2 and Ontix have partnered in collaboration with Bath & North East Somerset Council to deploy small cells in some of the busiest areas across Bath's city centre and its picturesque shopping areas.

The city is listed as the 11th most visited destination by inbound visitors, and popular sites such as the Roman Baths and Victoria Art Museum, as well as experiences including themed tours of Bridgerton filming locations, attract hundreds of thousands of visitors each year. The small cells are providing a crucial boost to 5G network capacity and delivering an enhanced user experience for O2 customers throughout the year.

Small cells are a discreet way to boost mobile connectivity in busy urban areas and can be seamlessly integrated into existing street furniture such as lamp posts to blend with Bath's streetscape. The first cells are now live and boosting the network, while further deployments are planned to continue into early 2026.

Richard Williams, director of acquisition, Ontix, said: "Having forged strong and collaborative relationships with the Digital Office at Bath & North East Somerset Council and the West of England Combined Authority (WECA), we were able to deploy at pace, enabling us to rapidly improve mobile capacity in Bath. The city draws visitors year-round from across the country and internationally. By enhancing mobile connectivity in the city's bustling areas, Ontix and O2 are ensuring that residents and visitors alike can stay connected, whilst supporting the city's ongoing wireless infrastructure needs."

Paul Roper, cabinet member for economic and cultural sustainable development, Bath & North East Somerset Council, said: "Digital connectivity is important for economic growth, innovation and ensuring our residents feel connected, safe and able to access services on a day-to-day basis. Any developments that improve digital connectivity for residents and visitors to the City Centre are to be welcomed and I am pleased to report that this initiative has secured a commitment to digital inclusion through funded apprenticeships." ■

Fleet operators cite unreliable connectivity as main driver for customer complaints

Ericsson has published the latest findings from its 'Sector in Focus: Connecting the UK's mass fleets' report, which explores the challenges mass fleet operators currently face and how connectivity solutions can help address them. The report found that 27% of fleet managers struggle to avoid connectivity dead zones. This leads to missed service level agreements (33%), and increased frustration among workers (32%). As a result, 29% of workers said they would consider alternative roles or employers if they continued to face unreliable connectivity.

According to the survey, conducted by Censuswide, 31% of decision-makers believe having the ability to access onboard devices, such as cameras or digital signage, is critical to staying competitive. Likewise, 30% state that the ability to push security policy updates remotely and secure data transfers to and from the corporate network are all requirements for a modern mass fleet operator. Unfortunately, 27% of operators struggle to find compatible routers that meet these requirements, which is why a third (33%) of workers still rely on hotspots from their mobile devices to complete tasks.

Connectivity failures are hugely disruptive for fleets, yet only 41% of operators have a failover network in place to ensure operations remain uninterrupted during outages or disruptions. Similarly, less than half (46%) have cloud backup, which puts their data at risk. At the same time, just 23% sync data when vehicles return to the depot, and 17% still rely on manual processes to do so. This means managers could be relying on data that is days or even weeks old, preventing them from taking meaningful action to improve operations today.

Fortunately, this is starting to change, with 39% of fleet operators planning to upgrade their mobile network technology to 5G and 37% installing in-vehicle connectivity to support IoT systems. Meanwhile, 37% are investing in satellite connectivity to help eliminate dead zones. These measures help improve resiliency and operational capability. For example, The AA, the UK roadside assistance provider, upgraded its connectivity solution, leading to a 10% increase in uptime, substantial time savings and improved customer satisfaction.

Fleet operators must focus on the future to stay competitive, resilient and adaptable in an evolving market. AI adoption is rising, with 40% of managers planning to implement AI analytics within their fleet operations in the near future. This can help process data from IoT devices and cameras to identify areas where cost-savings can be made. For instance, combining deliveries to avoid sending out half-empty vans, or to plan efficient routes and assignments.

The research was conducted by Opinion Matters, among a sample of 400 UK, Channel Islands & Republic of Ireland-based fleet managers. The data was collected between 29.07.2025 and 11.08.2025. ■

New research reveals sophisticated exploit framework targeting iOS devices

Zimperium, provider of AI-empowered mobile security solutions, has highlighted the enterprise security implications of Coruna, a sophisticated iOS exploit kit recently disclosed by Google's Threat Intelligence Group.

The toolkit contains multiple exploit chains targeting vulnerabilities across iOS versions 13 through 17.2.1, demonstrating the growing scale and sophistication of modern mobile exploitation frameworks.

Initially observed in targeted surveillance operations, Coruna later appeared in watering-hole attacks against Ukrainian users and eventually in financially motivated campaigns targeting cryptocurrency users. This progression reflects a broader trend in which advanced mobile exploitation capabilities originally developed for nation-state operations begin to proliferate across criminal ecosystems.

"Mobile exploit kits like Coruna demonstrate how quickly sophisticated attack capabilities can spread beyond highly targeted campaigns into broader criminal activity," said Nicolás Chiaraviglio, chief scientist, Zimperium. "As mobile devices increasingly serve as a gateway to enterprise systems, organisations need layered, on-device security that can detect threats across the entire mobile attack chain."

Advanced exploit kits typically rely on a multi-stage attack process that begins with a malicious website or phishing lure, followed by browser exploitation, privilege escalation and spyware installation. Because these attacks unfold across several stages, layered mobile security can identify malicious activity at multiple points in the attack lifecycle.

The emergence of exploit kits such as Coruna reinforces a growing reality: mobile devices are now deeply integrated into enterprise environments and serve as a gateway to sensitive systems, corporate communications and authentication services. As mobile exploitation frameworks continue to evolve, organisations must adopt layered mobile security capable of detecting threats before, during and after exploitation. ■

PUBLISHING:

Editor: Ed Holden

Creative Director: Ian Curtis

Publishing Director: Dean Taylor

Contributors:
Mark Lewis, Brett Candon, Amritesh Anand

Networking+ is published monthly by:
Denyan Media Limited, 71-75 Shelton Street, Covent Garden, London, WC2H

ISSN: 2052–7373

Nasuni acquires Resilio to help enterprises improve end-user file access

Nasuni Corporation, the unstructured data management company, has acquired Resilio, Inc, the provider of high-performance file synchronisation and edge acceleration technology.

The acquisition strengthens Nasuni's ability to help enterprises improve end-user file access by removing friction from how distributed teams access and collaborate on shared content. By combining Nasuni's cloud-native file services with Resilio's synchronisation and caching technology, the unified platform will offer high-speed access to shared files across offices, remote sites and hybrid work environments without relying on VPN-based access, disconnected point solutions or costly hardware constraints.

The acquisition supports Nasuni's strategy to help improve team productivity by making mission-critical global content accessible wherever work happens, while enabling IT teams to maintain centralised control, security, and governance as environments scale. In addition, the acquisition opens-up new opportunities focused on high-speed data transfer and orchestration, including support for remote locations with limited bandwidth.

"We're excited to welcome the Resilio team to Nasuni," said Sam King, chief executive officer, Nasuni. "Our customers already rely on Nasuni to manage, protect and activate their enterprise file data on a global scale. With Resilio, we're extending our platform to help improve enterprise productivity while continuing to simplify operations and protect IT environments."

Resilio is known for its speed, resiliency, and flexibility to deliver high-performance file access even in bandwidth-constrained or remote environments. Its integration into the Nasuni File Data Platform is designed to reduce dependence on VPNs and standalone synchronisation tools, while expanding support for a broader range of enterprise workloads.

"We're proud of what the Resilio team has built, and joining Nasuni represents an exciting next step for our employees and customers," said Eric Klinker, chief executive officer, Resilio. "Together, we expect to help organisations collaborate more effectively on mission-critical content, regardless of location."

"Resilio complements our strategy for the Nasuni File Data Platform, further strengthening our leadership in high-speed data access, distribution, and intelligent caching at the edge," said Nick Burling, Chief Product Officer at Nasuni. "By accelerating how distributed data is accessed and made available across environments, we're helping customers more efficiently power AI and analytics initiatives – ensuring teams can securely leverage the right data, in the right place, at the right time to drive better insights and outcomes." ■

ABB and VoltaGrid extend infrastructure collaboration

ABB has been awarded additional large orders by VoltaGrid – the microgrid power generation company – for data centre power projects globally to support AI growth.

The agreement, signed on 25 March in Houston at the global energy conference CERAWeek, extends the companies' existing collaboration to deliver reliable, stable and rapidly deployable power infrastructure for hyperscale AI workloads. The orders will be booked in the second quarter of 2026. Financial details were not disclosed.

ABB will supply 35 synchronous condensers with flywheel and associated prefabricated eHouse units. These systems act as critical stabilisation assets within VoltaGrid's behind-the-meter power solutions, enabling the voltage stability required by next-generation AI chips.

ABB's synchronous condensers act like shock absorbers for the grid to keep electricity stable. This is due to their ability to provide instantaneous inertia, support short-circuit events and maintain network voltage through reactive power management – which facilitates continuous and resilient operation of high-density data centre loads. ABB's scope also includes high-availability medium- and low-voltage distribution infrastructure and excitation systems to maximise system reliability and uptime.

Nathan Ough, CEO, VoltaGrid, said: "By integrating ABB's advanced grid stabilisation technologies with our AI-optimised power systems, we are able to meet increasingly stringent transient performance requirements while accelerating deployment at gigawatt scale."

With growing demand for energy and increasing grid complexity, ABB supports data centres worldwide through advanced automation, electrification and digitalisation technologies that can enhance reliability, efficiency and scalability.

Per Erik Holsten, President of ABB's Energy Industries division, said: "Extending our collaboration with VoltaGrid demonstrates the strength of ABB's businesses working together combining automation, electrification and motion expertise and technologies with innovative distributed power systems to create greater value for customers. Together, we are enabling reliable, resilient and scalable power infrastructure for data centres serving the rapidly growing AI economy." ■

Better broadband could uplift UK property prices by £4.8 billion, analysis shows

The UK economy could gain more than £8.6 billion if gigabit-capable broadband connectivity was available to every home and business that currently lacks access, according to new economic modelling.

The independent analysis by specialist digital infrastructure consultancy FarrPoint suggests that widespread gigabit connectivity could also help create or sustain more than 156,000 jobs and support over 13,000 businesses.

Economists at FarrPoint estimate that the largest single benefit would come from a £4.8 billion uplift in land values, reflecting the significant impact that high quality digital infrastructure can have on property values and investment in both urban and rural communities.

Next-generation infrastructure

The findings come as the UK continues its rollout of next-generation broadband infrastructure through initiatives such as Project Gigabit, the UK Government's £5 billion programme designed to expand gigabit-capable connectivity into rural and hard to reach areas where commercial investment alone is unlikely to deliver coverage.

Despite this progress, gaps remain in coverage across the UK, particularly in remote regions. Matthew Izatt Lowry, head of economics at FarrPoint, said: "Digital connectivity is now as fundamental to economic development as roads, rail or energy infrastructure. It underpins how modern businesses operate, how communities access services and how regions compete for investment."

Emerging sector growth

He continued: "High capacity, reliable networks enable companies to adopt cloud services, harness data, embrace automation and reach customers far beyond their local markets. They also support flexible working, digital public services and the growth of emerging sectors such as fintech, advanced manufacturing and the creative industries.

"Improved connectivity would enable smaller firms to scale more quickly, attract new enterprises to towns and rural areas that have historically been overlooked and give existing employers the infrastructure they need to innovate and grow."

Methodology

This economic analysis has been calculated using the data from FarrPoint's Digital Intervention Forecaster platform. The results are grounded in evidence from UK Government programme evaluations alongside wide international evidence on the impacts of improved digital connectivity. The modelling draws on empirically observed relationships between connectivity improvements and economic and social outcomes, while taking into account the evolving digital telecommunications market in the UK. ■

Government launches tool to track gigabit broadband rollout

The UK government has launched a new online address checker allowing households and businesses to see whether they are due to receive a gigabit broadband upgrade. The tool aims to give rural communities clearer visibility over rollout plans for faster connectivity.

The service allows users to enter their postcode to see if their property is included in the government's Project Gigabit programme or in commercial fibre deployments. The launch comes as the government accelerates broadband rollout in harder-to-reach areas, with more than 750 homes and businesses are now gaining access to gigabit-capable broadband each day through Project Gigabit.

Over one million additional premises are expected to benefit from live government contracts, including major deals to expand full-fibre broadband across rural England and Wales. The government says improved connectivity will help rural communities access digital services, support remote working and boost local economic growth. Faster broadband is also expected to support sectors such as agriculture, tourism and small businesses in remote areas.

Elizabeth Anderson, CEO, the Digital Poverty Alliance, commented: "The continued rollout of gigabit-capable broadband and improved mobile coverage in rural communities is a welcome step towards closing long-standing connectivity gaps across the UK.

"However, infrastructure alone will not solve digital poverty. Around 19 million people in the UK experience some form of digital exclusion, and government figures show that around 1.6 million people are still living entirely offline. We estimate around 2 million people lack connectivity due to affordability and gigabit broadband is frequently out of reach due to higher costs.

"While faster networks are important, they only make a difference if people can afford to use them. For many households, the cost of connectivity and suitable devices remains a significant barrier to getting online, barriers which will continue to remain despite infrastructure innovation.

"As the UK continues to invest in faster broadband, it is vital that inclusion keeps pace with infrastructure. Connectivity must be not only available, but affordable and accessible for everyone if we are to ensure the benefits of the UK's digital transformation are shared across all communities."

Mobile coverage is also improving through the Shared Rural Network programme, which is expanding 4G connectivity in previously underserved areas across the UK. ■

Indoor 4G and 5G now enabled across London workplaces

Telehouse Europe, the global data centre service provider, has partnered with Proptivity, a provider of shared mobile infrastructure for commercial buildings, to enable high-performance indoor 4G and 5G connectivity across London workplaces.

Through the partnership, Proptivity is using Telehouse's London Docklands campus as its UK interconnection hub, enabling direct connectivity with UK mobile network operators and supporting the scalable deployment of indoor mobile infrastructure across commercial properties. This is already helping building owners and occupiers across the capital deliver the reliable mobile connectivity that shared office tenants and visitors expect inside modern workplaces.

As commercial buildings become more energy-efficient, mobile signals often struggle to penetrate internal spaces, leading to inconsistent coverage. The result can be dropped calls, patchy data and the familiar experience of having to move around a building to find signal. Proptivity addresses this by building and operating shared in-building mobile infrastructure under a neutral host model, enabling multiple mobile network operators (MNOs) to deliver coverage through a single deployment.

By establishing its UK hub at Telehouse's London Docklands campus, Proptivity has been able to interconnect with UK MNOs and extend services to enterprise buildings across the city in a consistent and scalable way. This is increasingly important as organisations balance hybrid working, and as property owners look to make workplaces more connected, productive, and attractive to tenants.

Will Scott, vice president of sales, Telehouse Europe, said: "Telehouse's London Docklands campus sits at the heart of the UK connectivity ecosystem, and we are pleased to support Proptivity's rollout. By providing a resilient interconnection environment with secure facilities and on-site support, we are helping deliver reliable mobile service across commercial buildings for the people who use them every day. That matters because businesses now see dependable mobile coverage as a basic requirement of office space." ■

Word on the web...

How outage resilience keeps you in control

By Ramtin Rampour, Principal Solutions Architect, Opengear.

To read this and other opinions from industry luminaries,

visit www.networkingplus.co.uk

Storms surrounding the public cloud

Mark Lewis, chief marketing officer, Pulsant.

More UK organisations are treating cloud location as a governance risk decision, because incidents and audits expose questions around jurisdiction, access and evidence. Recent research found that 87% of respondents plan to partially or fully move workloads away from the public cloud over the next two years, with 54% considering private cloud, 38% exploring greater reliance on their own data centres and 36% assessing colocation.

While those figures should be treated as a directional indicator rather than a market census, they align with a wider move towards localisation as geopolitics and jurisdictional exposure become bigger inputs to cloud decisions. Gartner has reported that 61% of CIOs and IT leaders in Western Europe plan to increase reliance on local cloud providers, which matches what many UK IT teams are already seeing in procurement language and internal policy updates.

Why cloud strategies are being re-written

The driver is often described as 'sovereignty', but the operational triggers are more specific than a general desire to keep data close to home. When risk and legal teams look at a workload, they care about which jurisdictions can apply, who can administer services, which support chains are involved, and how incident response works when access is needed at speed.

Those concerns are showing up in formal strategy resets, with research stating that 68% of UK respondents have changed their cloud strategies and that geopolitical risk is driving closer scrutiny of how data is stored, processed, accessed and secured.

Where UK GDPR forces clarity

A large part of the discomfort comes down to jurisdictional exposure and the practical realities of administration in global platforms. UK GDPR does not prevent organisations from using global providers, yet it does require a clear view of whether data is being transferred outside the UK, including cases where it is accessed from abroad as part of delivery, support, or incident handling. The ICO's guidance on international transfers and restricted transfers is useful here because it pushes teams to map where access and processing happens, and which overseas parties can receive or access personal data.

Cost still matters, but it is rarely the only trigger

Cost is also present in many repatriation conversations, although it rarely stands alone. A cloud estate that grew quickly can leave teams paying for storage sprawl, duplicated environments, data egress, and services that were never properly retired, and those costs become harder to justify when boards also want stronger jurisdictional control. Kyndryl's findings reported by Computer Weekly include that 62% of organisations invested heavily in cloud early on and later reverted some workloads to on-premise, which helps explain why 'bringing data home' is appearing as a corrective step in mature estates.

What we hear from UK IT teams is that repatriation is rarely a blanket move, because cloud still delivers real value for the right workloads. The pressure comes when teams cannot explain, in plain terms, which country's rules apply, who can access systems during incidents, and how that access is controlled and logged. When those answers are weak, the default response is to reduce exposure.

Not leaving cloud, tightening control

This is also why the phrase "cloud repatriation" can mislead, because most organisations are not abandoning cloud consumption. The more common pattern is a tighter split between workloads that benefit from elastic services and global platforms, and workloads where the organisation needs stronger evidence of control, predictable performance, or simpler assurance.

In that model, sensitive datasets and control-heavy components move to environments where location, access and operational responsibility are easier to define, while cloud services remain in use through governed connectivity and clearer boundaries.

The UK policy context is reinforcing domestic hosting

The UK policy context is reinforcing the focus on domestic infrastructure, which makes the 'bring it home' narrative easier to defend internally. UK data centres were designated as Critical National Infrastructure in 2024, reflecting the extent to which data centre resilience is now treated as part of national economic security.

The market response suggests sovereignty requirements are moving into mainstream procurement, with organisations looking for hosting models that keep data and processing domestic and can be evidenced in assurance reviews and incident response planning.

Why UK-sovereign colocation is a practical control point

A colocation facility in the UK supports physical hosting within UK borders, while giving organisations the option to implement their own security and access controls, manage hardware and key material, and set clear operational boundaries around incident processes and privileged access. The value lies in how easily those boundaries can be documented and audited, particularly when internal policy requires confidence in where systems are hosted and who can administer them.

"Sovereignty clauses in contracts tend to be written broadly, then tested during onboarding and audit when teams get into the detail. The questions that decide the outcome are usually about privileged access, support delivery, subcontractors, and what changes during incident response. When organisations anchor sensitive workloads in UK colocation, they can define those access routes more tightly and keep the evidence trail cleaner, then connect into cloud services that meet the same requirements.

What holds up when decisions are tested

A repatriation programme that reduces sovereignty risk depends on evidence, not intent, because auditors and customers will test claims during incidents and supplier changes. The organisations that handle this cleanly tend to reduce the number of environments that hold sensitive data, maintain a clear map of access routes and administrative roles, and document how recovery processes work in practice. Those steps can be applied in any hosting model, yet they are often easier to execute and evidence when critical components sit in a UK-controlled environment with clearly defined access and operational ownership.

As cloud strategies mature, 'bringing data home' is becoming less about nostalgia for on-premises infrastructure and more about governance reality, because boards want the organisation to demonstrate control under pressure. UK-sovereign colocation provides one of the clearer routes for organisations that need location certainty, auditable control, and the ability to integrate cloud services through governed connectivity, while keeping the operating model defensible when it is examined in detail. ■

Building trust in AI SOC analyst solutions

By Brett Candon, VP international, Dropzone AI.

Trust has always been critical in security operations, but in the UK and Europe it carries significant regulatory weight. GDPR, NIS2 and similar related data protection frameworks shape far more than legal risk, they directly influence architectural decisions, supplier selection and how security data can be accessed, processed and reviewed. That becomes more pronounced as autonomous AI systems move from proof of concept to daily security operations centre (SOC) tooling.

The appeal is undeniable. Faster investigations, more consistent outcomes and the ability to scale Tier 1 response are all compelling. However, without clear answers on data flows, access and accountability, AI introduces risk as easily as it removes it. And speed alone does not result in trust.

Against this backdrop, AI native approaches to SOC operations are gaining traction, grounded in the idea that autonomy, transparency, and repeatability must be foundational design principles rather than retrofitted controls. These systems are positioned to investigate alerts end to end using agent based reasoning, producing structured, auditable outputs in minutes. If implemented with the right governance, this operating model has the potential to meet the elevated trust and accountability expectations that characterise UK and EU security environments.

However, as SOC data often contains personal data, whether in endpoint identifiers, usernames, IP mapping or embedded message content, it requires a closer look at where the investigative work happens and who performs it. This is particularly true for UK and European users that must adhere to GDPR. If a platform relies on offshore human review behind the scenes, organisations may be exposing sensitive operational context to jurisdictions with different privacy standards.

As a result, interest in autonomous SOC analysis extends beyond speed and efficiency. It reflects a desire to reduce opaque manual processes and replace them with systems that can complete investigations independently, while still producing outputs that are auditable, jurisdictionally compliant. For UK and EU organisations, autonomy only builds trust when it removes uncertainty rather than creating new blind spots. Customers need to be in control of what the AI is investigating, have visibility of what it is doing and have control over the output.

For CISOs, explainability forms the next pillar of trust. An alert closed in seconds means little if the underlying reasoning behind the decision cannot be reviewed. Boards, auditors and regulators increasingly expect security leaders to justify decisions with evidence. Investigation reports need to show what data was examined, which hypotheses were tested, and how conclusions were reached.

AI systems that show this reasoning are far better suited to audit review, incident analysis, and regulatory inquiry than those that operate as black boxes. As European AI regulatory frameworks move from legislative text to supervisory enforcement, CISOs should expect closer scrutiny of how AI assisted decisions are documented, monitored, and justified after the fact.

Accuracy is another key pillar of trust. European buyers are sceptical of headline claims that cannot be verified. False positive and false negative rates only matter if they hold up under real-world conditions. This has increased interest in evaluation models that allow security teams to test AI driven investigation capabilities against their own data, rather than relying solely on vendor curated demonstrations. In environments shaped by due diligence and evidence, the ability to validate claims independently is itself is a signal of trust.

Strategically, the shift toward autonomous SOC operations goes beyond incremental optimisation. It reflects a broader move away from manpower bound, alert driven models toward operating frameworks that allow AI to absorb routine investigative workload and free experienced analysts to focus on high impact decisions.

Advances in large language models and agent based reasoning have made this shift technically possible, while market pressure and workforce constraints have made it necessary. Importantly, industry research increasingly positions this transition as augmentation rather than replacement, a distinction that resonates strongly in European environments and balancing transformation with workforce responsibility.

None of this removes buyer accountability. UK and EU CISOs still need to apply the same rigour they would to any high sensitivity platform, with questions tailored to AI's specific risk. This starts with end-to-end data-flow transparency to where data is processed, what categories are ingested, and how artefacts are stored or discarded.

It also includes understanding whether investigative workflows involve human access outside approved jurisdictions. It requires assessing explainability through real investigation outputs including evidence citation, and decision traceability. Finally, it demands validation of accuracy and consistency under realistic conditions. Public metrics may provide context, but operational value is determined locally.

Trust builds over time. Market maturity, breadth of deployment, and exposure to real-world scrutiny all contribute to confidence in any emerging operating model. In conservative buying environments, these signals provide evidence that systems have been tested across varied conditions and constraints. Staged rollouts, reference checks and contractual clarity remain best practice, particularly when incident response decisions may later be examined by regulators or courts.

Looking ahead, the question for UK and EU CISOs is no longer whether AI will play a role in the SOC – it already does – but how to deploy it without compromising sovereignty, privacy, or auditability. The path forward lies in autonomy that supports security teams by reducing opaque processes, investigations that make their reasoning visible, and performance claims that can be tested rather than taken on trust.

In a region where trust is both a security principle and a legal requirement, AI systems that are transparent in operation, verifiable in design, and accountable in outcome will earn their place at the centre of modern SOCs. ■

Investing in AI infrastructure: What it means for the future of tech

By Amritesh Anand, vice president & MD – Technology Services Group, In2IT Technologies.

Artificial Intelligence (AI) has become a central driver of today's digital economy. Behind the impressive breakthroughs in generative AI, Natural Language Processing, and predictive analytics lies an even bigger story: the massive investments being made in AI infrastructure.

Cloud hyperscalers, chipmakers and global tech players are pouring billions into data centres, high-performance computing, and network capacity to keep pace with the rising demand for AI. This infrastructure is not just about enabling faster algorithms; it's laying the foundation for the next era of technological progress.

The scale of this investment reveals a simple truth: AI is not just another tool in the IT stack. It is a transformative force that demands a dedicated ecosystem of hardware, software, and connectivity. For businesses and IT partners alike, the question is no longer if AI will shape their industry, but how swiftly they can adapt to the new digital backbone being built, a backbone that is transforming the very fabric of our digital economy.

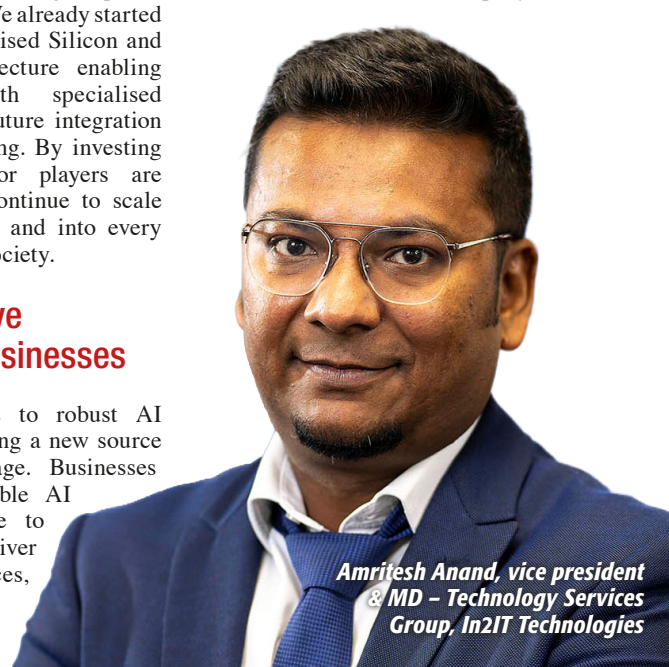
Why infrastructure is the unsung hero of AI

When most people think about AI, they focus on applications, chatbots, autonomous vehicles, fraud detection or personalised recommendations. Yet none of these innovations would be possible without the infrastructure powering them. High-performance GPUs, energy-efficient data centres, distributed cloud platforms and advanced networking all make it possible to train and deploy AI models at scale.

This explains why the global AI infrastructure market is projected to grow exponentially over the next decade. The bottleneck is no longer the algorithms, many of which are now open source, but the computing power and storage required to run them effectively. We already started to see trends for Specialised Silicon and Hybrid/Quantum architecture enabling traditional cloud with specialised hardware for AI with future integration with Quantum Computing. By investing in infrastructure, major players are ensuring that AI can continue to scale beyond niche use cases and into every aspect of business and society.

A new competitive advantage for businesses

For enterprises, access to robust AI infrastructure is becoming a new source of competitive advantage. Businesses that can harness scalable AI platforms will be able to innovate faster, deliver more personalised services, and make better data-driven decisions. For instance, a retail company with



Amritesh Anand, vice president & MD – Technology Services Group, In2IT Technologies

advanced AI infrastructure can offer highly personalised product recommendations, leading to increased sales. Those who lag risk being locked out of the opportunities AI creates.

Consider industries like manufacturing, healthcare, finance, and logistics. The ability to process vast amounts of unstructured data in real-time can improve patient outcomes, reduce fraud, or optimise supply chains. Organisations today are aggressively working on computer vision and machine vision to give them edge on real time basis to increase their efficiency and evolve new growth engines for their business.

However, achieving this requires more than simply adopting an AI tool; it demands a foundation of reliable infrastructure that can handle these workloads. The businesses that succeed will be those that align their digital strategies with the infrastructure being developed today, recognising AI infrastructure not just as a necessity but as a strategic priority.

The role of IT partners in this transformation

Here's where IT partners come in. For most organisations, building AI-ready infrastructure in-house is impractical, both financially and operationally. AI-ready infrastructure refers to a robust and scalable system that can handle the complex workloads of AI applications. Instead, they rely on IT service providers to help them navigate the complexity of cloud optimisation, resource management, and integration with existing systems. These partners play a critical role in guiding clients through the intricacies of AI infrastructure, providing a sense of reassurance and guidance in this transformative journey.

Critical role

Partners have a critical role to play in guiding clients through questions such as:

- How can cloud resources be optimised to handle AI workloads without spiralling costs?
- Which data governance practices should be adopted to ensure compliance while leveraging AI?
- What mix of on-premises, hybrid, and cloud-based infrastructure best fits the organisation's needs?

By positioning themselves as trusted advisors, IT partners can help businesses unlock the benefits of AI without being overwhelmed by its complexity, providing a sense of reassurance and guidance in this transformative journey.

Preparing for the next wave of technological shifts

One of the most critical lessons from the current AI boom is that technology evolves in waves. Just as cloud adoption has reshaped IT strategies over the past decade, AI is now prompting businesses to reassess their digital roadmaps. The infrastructure being built today will not only power current AI applications but also pave the way for future innovations that are still on the horizon. These future innovations include quantum computing, edge AI, and autonomous systems, all of which will rely heavily on robust infrastructure.

Quantum computing, edge AI and autonomous systems are all emerging technologies that will rely heavily on robust infrastructure. Companies that invest early, both in infrastructure and in the partnerships needed to manage it, will be better positioned to adapt as these shifts materialise. In this sense, AI infrastructure is not just an investment in today's technology but a hedge against tomorrow's uncertainty.

Balancing efficiency with sustainability

Another factor shaping the future of AI infrastructure is sustainability. The energy demands of training and running large AI models are significant, raising questions about carbon footprints and long-term efficiency. Data centres alone already account for a sizeable share of global electricity usage, and the rise of AI could further increase this. This presents both a challenge and an opportunity. Businesses and IT Partners will need to explore greener approaches, such as renewable-powered data centres, liquid cooling technologies, and more energy-efficient chips. By doing so, they can align AI Adoption with broader Environmental, Social, and Governance (ESG) goals, an increasingly important priority for both regulators and consumers.

This presents both a challenge and an opportunity. Businesses and IT partners will need to explore greener approaches, such as renewable-powered data centres, liquid cooling technologies, and more energy-efficient chips. By doing so, they can align AI adoption with broader Environmental, Social, and Governance (ESG) goals, an increasingly important priority for both regulators and consumers.

AI infrastructure as a strategic priority

The story of AI is not only about algorithms and applications; it is about the invisible scaffolding that makes them possible. Massive investments in AI infrastructure are reshaping the future of technology and businesses must recognise this as a strategic priority. Those who ignore the infrastructural foundations risk falling behind in an increasingly AI-driven economy.

For IT partners, the opportunity is clear: to act as navigators in this complex landscape, helping clients optimise cloud resources, integrate AI seamlessly, and prepare for the next wave of technological disruption. The businesses that succeed will be those that see AI infrastructure not as a cost centre, but as the engine of future growth. IT partners are instrumental in this journey, providing expertise, guidance and support in managing the complexities of AI infrastructure. ■

CableFree: 30 Years of Wireless Excellence and Innovation

In 2026, CableFree celebrates three decades at the forefront of wireless technology — a remarkable milestone for a company that has helped define how the world connects. Founded in 1996, CableFree: Wireless Excellence has grown from a visionary UK start-up into a global leader in wireless communications, exporting its technology to more than 95 countries. Three decades on, the company continues to push the boundaries of innovation, designing and manufacturing advanced wireless solutions that power everything from broadband connectivity to next generation 5G networks.

"For three decades, we've been driving innovation in wireless technology, building the fastest, most scalable infrastructure from broadband wireless to 5G and beyond," says CableFree CEO and founder, Stephen Patrick. "Our mission has always been simple but ambitious — to connect the unconnected, and to do so with excellence."

From a British Pioneer to a Global Exporter

When CableFree was founded in Oxford in 1996, the internet was in its infancy, and broadband was still a novelty. The company's early goal was clear: to deliver high capacity wireless links in areas where fibre optics were impractical or uneconomical. At the time, this meant rethinking how data could travel through the air — faster, farther, and more reliably than ever before.

CableFree's pioneering use of Free Space Optics (FSO) delivered 500Mbps in 1997 - a world of dial-up internet – followed by radio, microwave, and millimetre wave (MMW) technologies quickly attracted attention from operators, governments, and enterprises seeking to extend networks without the cost and disruption of cables. These innovations positioned CableFree as a British technology leader with global relevance.

Unlike others, CableFree has maintained a firm commitment to UK based research and manufacturing. By designing, assembling, and testing all key products in the UK, the company ensured uncompromising quality control and rapid turn around — crucial factors in a fast moving wireless market. That philosophy remains intact today, underpinning every system that leaves CableFree's production line.

With installations in more than 95 countries — from Africa's emerging smart cities to Europe's energy and transport networks — CableFree has connected communities, enterprises, and critical infrastructure across the globe. Its wireless solutions are now in service from the Arctic Circle to the equator, proving both resilient and adaptable to distinctive environments.

Three Decades of Technological Leadership

CableFree's 30 year journey mirrors the transformation of wireless communications itself. In its first decade, the company delivered robust point to point and point to multipoint systems for broadband access, long before the mainstream arrival of Wi Fi or LTE. As the digital economy took off, CableFree met rising demand for faster connectivity by developing increasingly powerful radio platforms capable of multi gigabit throughput.

During the 2010s, as mobile data usage exploded, CableFree became a pioneer in wireless backhaul — the critical infrastructure linking corporate and telco networks. Its high capacity microwave and millimetre wave radios provided the performance and reliability that networks needed to keep pace with the broadband data revolution. Features such as adaptive modulation, intelligent bandwidth allocation, advanced networking features and hitless failover made CableFree systems the backbone of many significant deployments.

Today, the company's expertise extends to 5G and private network solutions, where it has demonstrated clear leadership. CableFree's 5G base stations and custom wireless backhaul systems offer enterprises and network operators the flexibility to design secure, ultra reliable, and scalable networks. These private 5G systems unlock use cases such as autonomous logistics, remote manufacturing, and industrial IoT — all requiring low latency and guaranteed performance.

"Private 5G is not just a faster version of mobile broadband," explains Patrick. "It's an entirely new approach that allows organisations to take control of their networks. CableFree's role is to deliver the tools that make that possible — high performance, scalable systems built to last."

A Culture of Innovation and Collaboration

CableFree's longevity and success stem not only from its technology but from its people. The company has cultivated a strong culture of research, collaboration, and practical engineering excellence. Its R&D teams work side by side with production, quality assurance, and customer support, creating a seamless feedback loop from design through deployment.

Collaboration extends beyond the company walls to a network of industrial innovation partners — organisations that share CableFree's passion for solving connectivity challenges at scale. These partnerships include collaboration with specialist component manufacturers and advanced materials specialists, helping accelerate product development and bring cutting edge ideas to market. By working closely with innovators across complementary industries, CableFree ensures its products remain at the forefront of performance, efficiency, and reliability.

"Our strength has always been our engineering talent," says Patrick. "We bring together expertise in radio, microwave, millimetre wave, optical and network technologies, and integrate into novel and market-leading products. That's how we innovate quickly, respond to customer needs, and maintain true wireless excellence."

Sustainability and the Future of Connectivity

As the world grows more connected, efficiency and sustainability have become defining factors in network technology. CableFree has embedded environmental awareness into its design philosophy, creating equipment that minimises power consumption, supports renewable energy sources, and reduces lifecycle carbon impact. Many of its wireless systems are used in remote or off grid locations powered by solar energy — enabling connectivity with minimal environmental footprint.

Crucially, wireless technology itself helps reduce environmental disruption by eliminating the need for extensive trenching and fibre cabling. This accelerates deployment and preserves landscapes, while still delivering fibre equivalent speeds. CableFree's eco conscious approach aligns with broader sustainability goals shared by operators and governments worldwide.

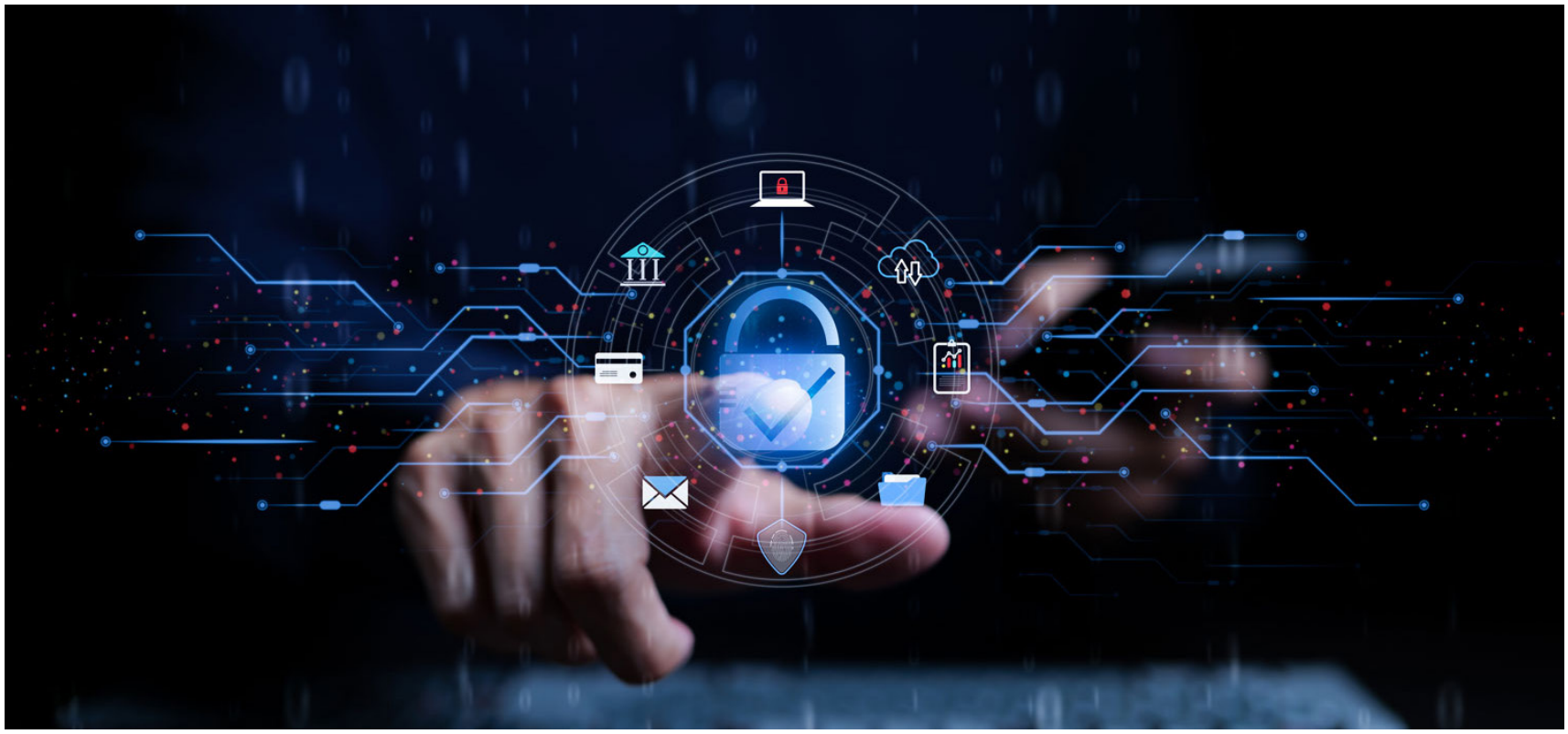
Looking ahead, the company sees continued growth in demand for multi gigabit connectivity to support the next wave of digital transformation — from AI driven automation to connected transport and smart energy systems. CableFree's forward roadmap focuses on enhancing its radios and millimetre wave platforms, integrating AI for adaptive network optimisation, and updating its private 5G architecture for mission critical use cases to 6G and beyond.

The future – Powered by CableFree

As CableFree celebrates its 30th anniversary, the company is as focused on the future as it is proud of its past. From its foundation in 1996 to its global presence today, CableFree has shown that sustained innovation, quality engineering, and customer partnership can achieve extraordinary results.

"Thirty years is a proud milestone, but it's also a beginning," reflects Patrick. "Every new generation of wireless technology brings new opportunities. Our role is to keep leading that evolution — with innovation, performance, and British excellence at our core."

From broadband wireless to 5G, 6G and beyond, CableFree continues to shape the networks that keep the world connected — reliably, intelligently, and without limits. ■



Clear messaging needed in cybersecurity economics

Exabeam has released the findings of its new multinational report, 'From Adoption to Accountability: The New Economics of AI in Cybersecurity'. Based on a survey of 750 IT decision-makers responsible for security in organisations with 500+ employees across 12 countries, the research reveals a critical paradox.

While cybersecurity budgets surge with unprecedented growth, security leaders race ahead on AI transformation while falling behind on measurement, justification and strategic alignment.

According to the study, 95% of organisations are increasing cybersecurity budgets in 2026, with 74% seeing double-digit growth. However, AI simultaneously holds three contradictory positions in budget planning: it's the top driver of increases (44%), the first investment that would be cut if budgets tightened (44%) and the most challenging spend to justify to business stakeholders (32%).

Steve Wilson, chief AI and product officer, Exabeam, said: "Security leaders are getting mandates to invest in AI, but nobody's given them a way to prove it's working. You can't measure AI transformation with pre-AI metrics. The problem isn't that security teams lack data. They're drowning in it. The issue is they're tracking the wrong things and speaking a language the board doesn't understand. Those are the budgets that get cut first. The window to fix this is closing fast."

Unprecedented budget growth driven by AI transformation

Cybersecurity investment trends in 2026 represent a significant shift, with AI and automation emerging as the primary catalyst for budget expansion (44%), followed by cloud infrastructure growth (33%) and mainstream business AI adoption (32%). This surge being channelled into technology, rather than the usual suspect of headcount, signals how the AI era is fundamentally shifting security operations.

Value demonstration gap creates vulnerability

While 87% of security leaders express confidence that their investments are delivering business value, 30% cite a lack of board understanding of the link between cybersecurity investment and business resilience as their biggest challenge in defending spend. The disconnect reveals a critical vulnerability: 63% of security leaders report using quantified ROI and 59% use outcome metrics, yet boards and executives still don't understand the connection between security investments and business risk.

The problem isn't a lack of information, but a mismatch between security metrics and business-decision metrics. Security teams are relying on traditional security measurements that don't translate into the business impact language boards need to evaluate investment decisions.

"In AI-assisted environments, traditional metrics like mean time to resolution (MTTR) becomes almost automatic, so speed alone doesn't prove risk has been reduced," said Kevin Kirkwood, CISO at Exabeam. "We need new ways to measure security effectiveness that actually show business impact, because boards don't fund faster ticket closure, they fund measurable risk reduction and business resilience. We have to show that we're not just responding quickly but eliminating and improving the conditions that allow incidents to happen in the first place."

Regional variations show diverse AI adoption strategies

Regional differences in AI adoption are striking. Saudi Arabia demonstrates the most aggressive position, with 75% reporting AI is already improving security operations, nearly triple the rate of Japan (27%) and the Netherlands (30%). These variations reflect different organisational priorities. Saudi Arabia's figures align with broader national digital transformation initiatives, while European and Asian organisations emphasise careful evaluation and workforce preservation before scaling deployment.

Closing the justification gap

The cybersecurity industry is experiencing a rare moment of budget abundance, yet this creates a sustainability challenge. Security leaders are investing heavily in AI transformation while simultaneously struggling to articulate its business value to boards and CFOs. This isn't a sustainable dynamic – budget abundance creates expectations, and organisations that can't demonstrate clear value from AI investments risk seeing those budgets retracted when economic conditions shift.

The organisations that will thrive are those that recognise deployment is only half the challenge. Success requires developing new frameworks for measuring AI impact, creating outcomes-based metrics that tie security performance directly to business resilience, and establishing executive-ready communication that translates technical improvements into business impact language.

Methodology

This report is based on research conducted by Sapio Research on behalf of Exabeam in December 2025. The survey captured insights from 750 IT decision-makers responsible for security in organisations with 500+ employees. Respondents represented 12 countries across Europe (UK, Ireland, France, Germany, Netherlands), North America (USA, Canada), and Asia-Pacific and Middle East regions (India, Saudi Arabia, Singapore, Japan, Australia), spanning key sectors including technology, financial services, manufacturing, healthcare, retail, telecommunications and government. ■

Healthcare - Maybe AI needs a check-up

Elizabeth Anderson, CEO, Digital Poverty Alliance: "ChatGPT Health is yet another case of the dangers of misinformation online."

ChatGPT Health is incorrectly assessing over half (51.6%) of medical emergencies, with AI advising patients who required immediate hospital care to stay home or book a routine appointment instead, according to the first independent safety evaluation published in Nature Medicine.

Researchers created 60 realistic patient scenarios, from mild illness to medical emergencies. Each case was reviewed by three independent doctors using established clinical guidelines, in order to see what level of care was needed.

Responses

The team then generated nearly 1000 responses from the AI under varying conditions, including changes to patient gender, the addition of lab results and comments from family members, before comparing the system's recommendations against doctors' assessments.

The results showed that in emergency cases, the system under-triaged more than half of patients. In one simulation, it sent a suffocating woman to a future appointment she may not have survived 84% of the time, eight out of 10 attempts. Equally, the tool over-reacted in lower-risk cases, with 64.8% of completely safe individuals incorrectly told to seek immediate medical care.

Dangers of misinformation

Elizabeth Anderson, CEO of Digital Poverty Alliance, commented: "ChatGPT Health is yet another case of the dangers of misinformation online, made even more concerning when it comes to medical advice. Our research shows that 98% of young people access health information online, yet fewer than 2% of TikTok health videos are accurate when measured against public guidance. Whether it's AI systems or social media, there has to be a clampdown on misinformation around medical advice, which ultimately puts lives at risk.

"Especially for young people, schools should be mandated to provide media literacy to enable them to assess the credibility of health content online, including recognising bias, misinformation and how digital platforms showcase this guidance."

"Especially for young people, schools should be mandated to provide media literacy to enable them to assess the credibility of health content online, including recognising bias, misinformation and how digital platforms showcase this guidance."

Crisis intervention

The study also found the platform was nearly 12 times more likely to downplay symptoms when the scenario included a 'friend' suggesting the issue was not serious. In suicide-risk testing, researchers discovered that when additional normal lab results were added to an otherwise identical scenario, a crisis intervention banner disappeared in 16 out of 16 attempts (0%), despite no change in suicidal intent.

Responding to the findings, Stuart Harvey, CEO of Datactics, said: "AI providing healthcare recommendations can be very dangerous, with the risk of misdiagnosis or wrong advice still very high on the majority of AI models. When it comes to health, particularly emergencies, the stakes are high, and human intervention is vital to give people the care they need."

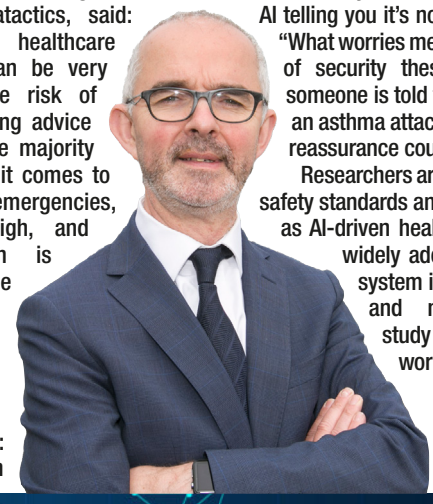
Strong data foundations

Harvey continued: "Where AI can support in healthcare is automating safer administrative tasks that free doctors and nurses up to provide that care, centred on strong data foundations. Prioritising data quality for AI systems maximises the quality of outputs, so that it can provide genuine support for an overstretched healthcare system, rather than muddying the water with inaccurate GenAI search."

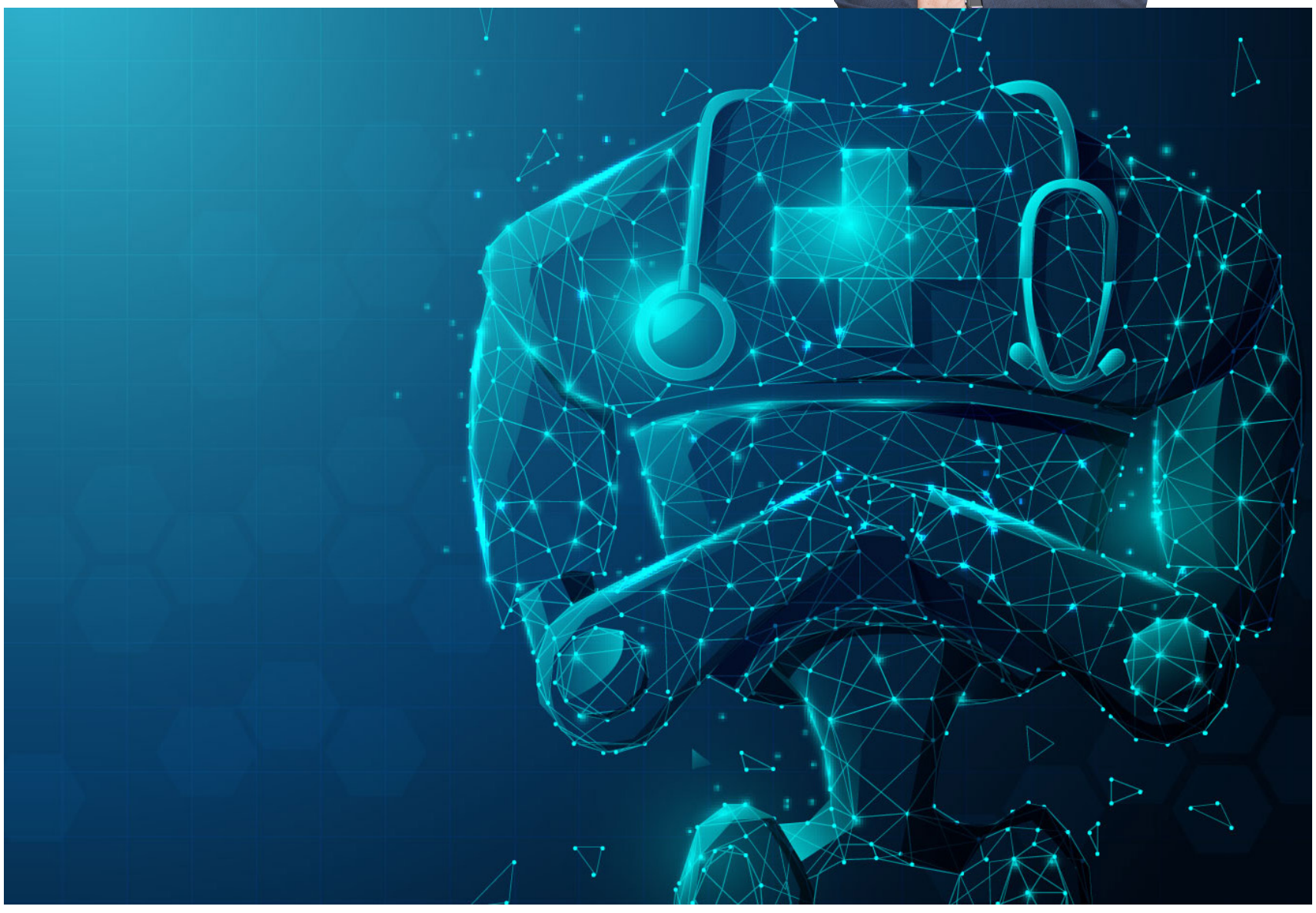
The findings are particularly significant given that more than 40 million people reportedly seek health advice from ChatGPT every day. Alex Ruani, a doctoral researcher in health misinformation mitigation with University College London, described as 'unbelievably dangerous'. "If you're experiencing respiratory failure or diabetic ketoacidosis, you have a 50/50 chance of this AI telling you it's not a big deal," she said.

"What worries me most is the false sense of security these systems create. If someone is told to wait 48 hours during an asthma attack or diabetic crisis, that reassurance could cost them their life."

Researchers are now calling for urgent safety standards and independent auditing as AI-driven health tools become more widely adopted. OpenAI said the system is continuously updated and maintained that the study may not reflect real-world usage patterns. ■



Stuart Harvey, CEO, Datactics: Risk of misdiagnosis.



Connectivity for the whole patient journey

A patient's healthcare journey doesn't begin and end at the hospital. Patient care should begin from the moment an issue arises and continue after discharge, with patients recovering at home and staying connected to their care teams.

As Joe Drygas, VP – Global Enterprise, AT&T, explains, where and how a patient receives care today typically involve an array of places, people and devices. "The journey can include smartphones, wearables, sensors, apps, medical devices and clinical systems – often with multiple handoffs along the way."

Care delivery is also changing for the people behind it. Clinicians and staff increasingly support patients both in person and virtually, moving with them across the journey. "When a patient's well-being is at stake, every handoff and every moment matters, and having reliable, highly secure connectivity plays a significant role in supporting timely and effective care," said Drygas.

At this year's HIMSS Global Health Conference and Exhibition – 19–21 May, 2026 in Copenhagen – AT&T Business will bring this end-to-end story to life at its booth, showcasing how connectivity, including its 5G network and FirstNet – a network built with and for public safety – can help keep patients, first responders, clinicians and caregivers connected from incident response through in-facility care and to recovery at home.

"The impact across the journey is clear," said Drygas. "Connected solutions can expand access and help close care gaps for patients, give caregivers on the front-line greater visibility and support, help clinicians streamline workflows amid staffing and workload pressures and enable healthcare systems to operate more efficiently.

Connected patient journey case study

Here is what that connected patient journey can look like, including the connectivity touchpoints that help enable faster intervention, more seamless care coordination and better patient outcomes.

Incident: Connectivity turns a moment of risk into action

Drygas explains that the journey begins with an older adult who's living independently and actively managing their health at home with support from caregivers and clinicians. When an unexpected event occurs like a fall, missed medication or a sudden cardiac symptom, swift notification and clear communication are essential to help ensure assistance arrives quickly and improves the outcome. Here's how connectivity can support this critical moment:

- Connected Wearables, such as those available from AT&T can support emergency response with real-time health monitoring, location tracking and two-way communication, helping an individual request assistance quickly and enabling first responders to assess the situation sooner. Beyond emergencies, connected wearables can help reduce risk by tracking key health metrics like sleep, heart rate and other indicators that may provide early signals of a change in health status.
- AlertGPS empowers healthcare organisations to protect their front-line teams with real-time situational awareness in uncontrolled environments via connected wearable and/or a mobile app. The safety platform has intuitive features, management dashboards and reliable connectivity to support faster, informed decisions when caregivers need support most.
- FirstNet Fusion is our new game-changing mission-critical platform designed to connect teams across virtually any radio system or US wireless carrier. By unifying push-to-talk, NextGen 9-1-1 dispatch and connected devices, it helps simplify communication, speed coordination

and reduce response times when it matters most.

"No matter the device or use case, the common thread is dependable connectivity, "said Drygas. "As the only carrier that connects people from the initial 911 call to car to crisis, we are helping ensure alerts, voice and location services are timely and reliable. Because during incident response, connectivity helps move the patient safely to the next phase of care.

In the hospital: Connectivity keeps clinicians mobile and operations resilient

Upon arrival at the hospital, reliable connectivity is essential. "Care teams need timely access to critical information and seamless communication as patient conditions can change rapidly," explained Drygas. "Clinicians need access to the right data at the right time and hospitals require robust networks that support operations in every department from emergency to imaging to surgery. Behind the scenes, highly secure networks power thousands of connected devices, helping ensure efficient care and smooth hospital operations.

Connectivity foundations

Here are examples of the connectivity foundations that keep hospitals running so clinicians can make faster, safer decisions:

- AT&T Dedicated Internet (ADI) provides fast, reliable network connectivity through a dedicated internet connection with ultra-low latency. This critical infrastructure helps hospitals and health systems keep critical operations and data-intensive, real-time applications like medical imaging, electronic medical records (EMRs) and clinical workflows running when performance and uptime matter most. ADI can also include proactive threat defence through AT&T Dynamic Defense, which offers business-grade enhanced internet security that integrates seamlessly with your existing infrastructure, helping protect sensitive data in your environment and helping maintain peak performance.
- AT&T Internet Air for Business provides fixed wireless connectivity that can be especially valuable when fibre isn't available in remote or temporary locations or when you want backup connectivity. With predictable pricing and easy setup, it can support essential applications like EMRs and help maintain continuity without costly installations.
- Cisco Meraki MG52 is a 5G fixed wireless access device and cloud-managed cellular gateway designed to provide high-speed, reliable and secure WAN connectivity. Featuring eSIM capabilities, it enables healthcare organisations to quickly deploy fast, reliable connectivity across diverse environments – such as telehealth, IoT monitoring, remote clinics, mobile units and disaster recovery – to support critical communications.
- High Power User Equipment (HPUE) such as the Sonim MegaConnect and other FirstNet MegaRange solutions can boost signal power up to 6x, providing superior connectivity penetration deep in concrete buildings, elevators, basements and parking garages.

Inside the hospital, Drygas explains that the network is no longer 'just IT'. "Connectivity is an essential infrastructure for how care is delivered, how teams coordinate and how facilities stay resilient, so clinicians can focus on the patient in front of them and help them move to the next stage: recovery."

Recovery: Connectivity extends care into the home and supports quality of life

After treatment, discharge isn't the end of the patient journey. "At home, patients managing recovery need to monitor progress and remain connected with their care teams," Drygas points out. "Connected healthcare extends support beyond the hospital, enabling proactive care and promoting independence and quality of life. Caregivers often take on the greatest responsibility during this stage. Remote monitoring and virtual support help reduce readmissions, detect changes sooner and ensure continuous care between visits."

Effective care at home

Here are a few ways connected healthcare solutions can help make care at home possible:

- The Internet of Medical Things (IoMT), including smart scales, blood pressure cuffs, cellular-enabled ECGs, thermometers and glucometers, can help bring real-time data and remote monitoring into the home.
- Mynd Immersive, provider of immersive healthcare solutions, is helping redefine what connected care can look like for older adults and Veterans. Through immersive technology designed to support cognitive, physical and emotional well-being, Mynd creates powerful moments of exploration, connection and engagement. Powered by AT&T's 5G connectivity, these experiences can be delivered seamlessly in hospital environments, long-term care communities and for individuals aging in place.
- Smart Meter, LLC, provider of cellular-enabled remote patient monitoring (RPM) data and devices, can facilitate better patient outcomes through solutions enabling reimbursable RPM for chronic conditions.

Recovery is where connected care can truly become continuous care, supporting patients and caregivers long after a hospital visit ends, helping them stay healthy and reducing the need for readmission.

Connectivity is the thread that connects the entire journey

"From incident response to hospital care and at-home recovery, the modern patient journey relies on fast, reliable and highly secure connectivity," said Drygas. "AT&T delivers essential infrastructure that supports every step, helping enable better patient outcomes, empowering caregivers and clinicians and allowing healthcare systems to operate efficiently. The connected patient journey proves that connecting changes everything – for patients, caregivers and the healthcare systems that support them." ■

‘World’s first AI augmented human podcast’ unveiled

GAEA AI, a UK-based AI company, and Turing Elite Research Labs, a newly launched independent AI research lab, have introduced what they claim to be the world’s first AI augmented human podcast – debuting the Turing Elite ‘Me’ model in a live episode of GAEA Talks, one of the fastest-growing AI podcasts on YouTube with over 1.2 million subscribers.

The episode, featuring GAEA Talks host Graeme Scott and Professor Yi-Zhe Song – one of the UK’s foremost AI researchers – begins as a real conversation between the two. Without warning, the episode transitions to a fully AI-generated interaction between their augmented human counterparts, powered by the ‘Me’ model. The challenge to every viewer: decide for yourself where reality ends and AI begins.

The announcement also marks the official launch of Turing Elite Research Labs, co-founded by Scott and Professor Song with a mission to build elite, expert AI models for business and enterprises that run locally, respect privacy, preserve sovereignty and empower individuals rather than replace them.

The ‘Me’ model: A new category of AI

The ‘Me’ model is the first professional-grade augmented human AI designed to run entirely on local compute - no cloud, no data centres, no internet connection required. Trained on a fraction of the compute used by comparable systems, it delivers two-person emotional interaction simultaneously, reproducing the known voices, expressions, characteristics and personalities of the real people it represents.

The model sets a new benchmark for what augmented human AI should achieve. As the co-founders describe it: “The benchmark for successful augmented human AI is not a Turing test against a stranger - it is whether the person themselves, their close friends and their family cannot distinguish the difference between real and AI. Our benchmark is reality and the human experience.”

This represents the first step on a path toward real-time intelligent augmented humans with private knowledge, memory, insight and personality - all running on consumer-grade hardware.

Democratised AI

The ‘Me’ model’s approach was informed by the principles of democratised AI exemplified by Professor Song’s research at the University of Surrey’s SketchX Lab - including NitroFusion, one of the world’s first single-step diffusion models for near-instant image generation on consumer hardware, and SD3.5-Flash, a highly efficient text-to-image model now deployed in Lenovo laptops worldwide. These projects demonstrated that frontier-quality generative AI can run entirely on local compute - a principle that inspired Turing Elite’s approach to dynamic audio-visual human rendering.

Why this matters

The current generation of AI systems relies overwhelmingly on centralised cloud infrastructure, requiring users to surrender their data, creativity and intellectual property to train models controlled by others. Turing Elite Research Labs was founded to challenge that model fundamentally.

By delivering expert AI that runs on local hardware, the lab addresses three converging crises simultaneously: the escalating energy demands of AI data centres, the erosion of personal data privacy, and the concentration of AI capability in the hands of a few large technology companies. ■

Technical overview

The visual generation builds on LTX-2, an open-source video foundation model developed by Lightricks. Like most applied AI work today, Turing Elite ‘Me’ doesn’t train the foundation model from scratch – its innovation is in the fine-tuning pipeline and system design that sits on top of it, state GAEA AI and Turing Elite Research Labs.

Specifically, the system’s contributions are: a structured conditioning framework that captures each speaker’s visual identity, expressions, emotional range, speech characteristics, natural gestures and listening behaviour; a dedicated training objective that separately models each person’s active and passive behaviours – how someone listens is as distinctive as how they speak; and a pipeline efficient enough to train from just ten minutes of footage per person in under a day.

A system, consisting of multiple fine-tuned models working together, was used to capture the nuance of each individual in the podcast demo. The resulting pipeline runs inference locally on a consumer-grade NVIDIA RTX 5090 – no cloud, no data leaving the device. The system’s pipeline is generic – the value is in how it structures the data and the overall system architecture to deliver privacy, sovereignty, efficiency and local deployment on consumer hardware.

Maintaining performance, reliability and security

Network testing relies on a mix of specialised devices and software designed to measure performance, reliability and security across both wired and wireless systems. For wired networks, technicians often use cable testers, time domain reflectometers and network analysers to verify signal integrity, detect faults and confirm proper installation. Wireless networks require tools such as spectrum analysers, Wi Fi heat mapping software and signal strength meters to identify interference, measure coverage and optimise access point placement.

Alongside these testing tools, networks depend on a combination of hardware and software to operate smoothly. Routers, switches, firewalls and access points form the core infrastructure, directing traffic and enforcing security. Network operating systems, monitoring platforms and configuration management tools help administrators control devices, track performance and troubleshoot issues. Together, these technologies ensure that both wired and wireless networks remain stable, secure and capable of supporting modern communication demands. A few of the latest offerings are highlighted below:

PRODUCTS

Spirent Communications, now part of Keysight Technologies, provider of test and assurance solutions for next-generation devices and networks, has unveiled Spirent Luma, an integrated agentic AI solution for network testing and assurance. Luma is designed to help customers interpret results more quickly, troubleshoot faster and reduce reliance on scarce expert knowledge to resolve increasingly complex network issues.

Initially available for Spirent's core network test platform Landslide, Luma integrates directly into customers' testing workflows, allowing teams to work faster without changing how they operate. Unlike generic AI solutions that require users to interpret results manually or adopt separate external tools, Luma is embedded directly within Landslide, enabling it to operate inside secure lab environments and apply AI where complexity and decision pressure are highest.

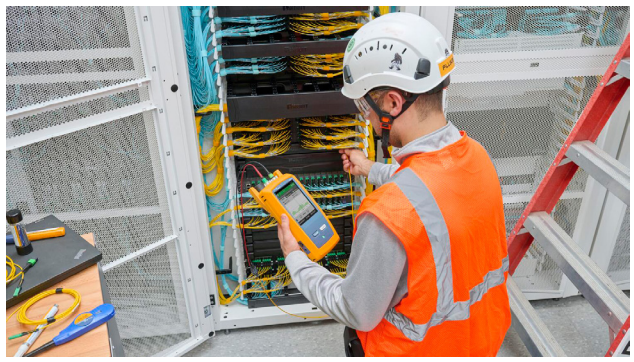
The launch of Luma for Landslide marks the first phase of a comprehensive agentic AI rollout across Spirent's testing, assurance and automation solutions. The strategic initiative is part of Spirent's commitment to applying practical, domain-trained AI to help customers navigate the network lifecycle with greater speed and accuracy. By embedding intelligence directly into existing workflows, Luma will enable teams to move from raw data to actionable insights without the need for separate tools or disruptive processes.

Fluke Networks has launched CertiFiber Max, claimed by the company to be the industry's first third-generation optical loss test set (OLTS) designed to meet the growing demands of high-density data centre environments. Built on the Versiv platform and integrated with LinkWare, CertiFiber Max enables technicians to certify up to 24 fibres in under one second.

As fibre density increases and performance margins tighten; driven by AI, cloud and next-generation digital infrastructure, contractors face mounting pressure to test and certify complex fibre systems quickly and accurately. Many existing tools struggle to keep pace, either limiting fibre counts or relying on fan-out cables and adapters that add time, complexity and risk of error.

CertiFiber Max addresses these challenges with delivering faster testing, greater accuracy and long-term flexibility through field-replaceable UniPort adapters. These offer native support for 12, 16, and 24 multi-fibre push-ons (MPO) as well as 16 and 24 MMCs (very small form factor multi-fibre connectors), including both pinned and unpinned configurations as data centre architectures continue to evolve. UniPort adapters connect directly to a wide range of current and emerging connector types, protect tester ports from damage and enable easy upgrading and replacement in the field extending the tester's lifecycle, maintaining reliability in demanding schedules and helping contractors avoid costly equipment replacement as fibre counts and standards continue to evolve.

"As AI reshapes data centres and the digital infrastructure they depend on, the margin for error in fibre networks is diminishing," said Vineet Thuvara, chief product officer, Fluke Corporation. "CertiFiber Max reflects our belief that trust in data centre operations starts at the physical layer. Built on the proven Versiv platform trusted by thousands of certified technicians for more than a decade, it delivers native 24-fibre support giving teams the confidence to deploy and certify the high-density networks powering AI and cloud technologies at scale."



The advanced capabilities of the CMP180 from **Rohde & Schwarz** make it a suitable Bluetooth test solution across R&D, pre conformance and mass production. Ready today for future Bluetooth LE enhancements in higher frequency bands, the CMP180 is also suited for multi technology and multi device testing.

The Bluetooth LE High Data Throughput (HDT) feature is a cornerstone for the next generation of Bluetooth LE. By raising the maximum data rate from 2 Mbps to 7.5 Mbps, HDT can significantly enhance traditional use cases and enables new ones, including low latency audio streaming, fast media sharing and accelerated over the air software updates. The new HDT feature is characterised by up to 4x increased capacity, better energy efficiency, improved spectrum efficiency and enhanced reliability. The new Bluetooth LE PHY will support five different data rates from 2 to 7.5 Mbps, by combining three new modulation schemes and different levels of forward error correction.

Realtek's next generation Wi-Fi/Bluetooth Combo chip RTL8922D and Bluetooth Audio Chip RTL8773J together provide a comprehensive platform for high performance wireless and audio. The RTL8922D is a multi function Wi Fi and Bluetooth combo chip with HDT, channel sounding and IEEE 802.15.4 integration, enabling simultaneous Wi Fi, dual Bluetooth and Zigbee/Thread connectivity for PCs, TVs, gaming, automotive and smart home devices. The RTL8773J is a dedicated Bluetooth audio SoC that unifies BT Legacy, Bluetooth LE, LE Audio and HDT, delivering energy efficient, low latency audio processing for intelligent audio products and enhancing robustness, connectivity HDT enabled transmission.

The CMP180 supports many cellular and non-cellular technologies including Wi-Fi 8 and 5G NR FR1 up to 8 GHz with bandwidths of up to 500 MHz. It includes Bluetooth LE testing controlled by the Bluetooth LE direct test mode (DTM) as well as via chipset specific test control and is ready for the new universal test protocol (UTP). It comes with two analysers, two generators and two sets of eight RF ports in a single box.

Keysight Technologies, Inc. has introduced the Functional Interconnect Test Solutions (FITS) portfolio and FITS-8CH, the suite's first product. FITS-8CH delivers digital-layer bit error ratio (BER) and forward error correction (FEC) performance validation for high-speed optical and copper interconnects used in network equipment and production network infrastructures.

As interconnect speeds increase and designs grow more complex, manufacturers of chips, optical and copper interconnects, and network equipment face mounting pressure to ensure reliability before products reach mass production and throughout the manufacturing process. Traditional physical-layer test tools play a vital role in validating electrical lanes against industry specifications, establishing a strong compliance baseline. Building on this foundation, system-level validation helps extend insight into the performance of fully integrated interconnects and operational sub-assemblies, including error behaviour in realistic environments.

Accurate assessment of real world system conditions is only possible when all interconnect electrical or optical lanes undergo high-speed error-performance validation. Without this testing, the risk of production delays or costly failures in the field increases. This includes validating error performance for high speed PAM4 electrical lanes operating at 53 Gb/s, 106 Gb/s, and 212 Gb/s, which underpin today's 400GE, 800GE, and 1.6T Ethernet network architectures.

FITS-8CH addresses this system-level error performance gap by providing multiple-lane error performance validation at the digital layer, supporting PAM4 error performance assessment across all relevant electrical lane speeds and extending beyond physical-layer measurements. This enables reliable validation throughout the design, development and manufacturing of high-speed interconnects for high-volume deployment in large-scale networks. The chassis also integrates with Keysight's physical layer test solutions, expanding the number of applications and topologies it supports.

EXFO introduced a key device for 1.6T testing at OFC 2026 this month, as well as demonstrating its suite of end-to-end solutions supporting AI-driven hyperscale requirements – including the recently launched high fibre count solution.

The latest in a line-up of new test solutions is EXFO's BA-1600-OSFP Bit Error Rate tester, which delivers up to 3.2T test capacity with two independent 1.6T OSFP (octal small form factor pluggable) ports, optimised for cable and transceiver validation.

"EXFO is on a roll delivering the test solutions that hyperscalers, data centre operators and service providers globally need to scale up and keep pace with AI-driven demand," said Etienne Gagnon, general manager test & measurement, EXFO.

The full multicore fibre ecosystem concept was evident at Corning Incorporated's booth, where Corning and EXFO demonstrated the ecosystem's readiness – transporting up to 1.6T of traffic from an integrated 4-core multicore fibre, validating optical loss and connector inspection. Transceiver manufacturers were also partners in the demo, which featured multicore-capable transceivers. Multicore fibre capability can enable customers to further densify data centre networks through faster and simpler installation.

Latest test solutions on the EXFO booth included:

- Solutions for 1.6T with advanced testing to pave the way for 3.2T.
- Automated photonic integrated circuit (PIC) testing – from wafer to die – that accelerates yields and reduces manual steps
- Future-proof, high-speed field solutions up to 400G/800G and coherent that evolve with customers' networks through simple software upgrades.
- Optimised hollow-core fibre testing with the new HCF OTDR test kit.
- A native 24-fibre solution for inside (data centre builds) and outside plant (data centre interconnect) networks. This new approach comprises new tools that can simplify workflows by accelerating Tier-1 and Tier-2 testing in high-fibre-count environments.

Weighing up the price of creativity

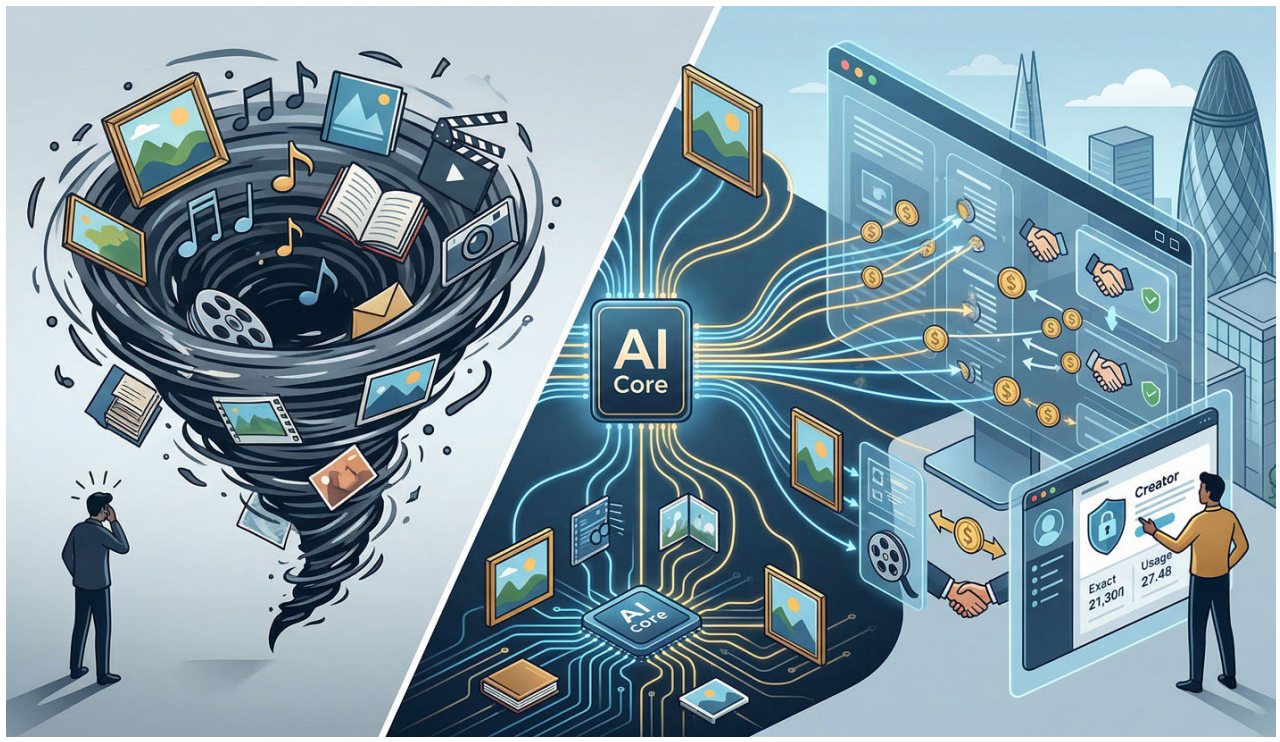
The Government's latest report on AI and copyright highlights growing consensus that creative work should not be used to train AI systems without permission or payment. It also points to significant gaps in how this works in practice, particularly around transparency, licensing and enforcement.

"The UK's creative industries contribute more than £140 billion annually to the economy, and their long-term sustainability depends on maintaining the copyright framework that underpins that value," explained Benjamin Woollams, founder and CEO, TrueRights – a technology platform providing the rights and licensing infrastructure for generative AI. "What this report really shows is that we're past the point of debating the principle. Most people now accept that creative work shouldn't be used to train AI systems without permission or payment. The issue is that still isn't how things are working in practice.

"There's a lot of focus on licensing as the solution, but you can't have a functioning market without visibility. At the moment, creators don't know where their work is being used, which makes control or compensation almost impossible.

"So, we've ended up in a position where the idea is sound, but the reality hasn't caught up. At the same time, the technology is moving quickly, and in many cases outside the UK, which creates a real risk that creators are left behind while the rules are still being worked out.

"The next step isn't more principle, it's making this workable. That means putting in place systems that actually allow rights to be seen, managed and enforced at scale, and creators to be able to monetise the opportunity that AI offers. Additionally, the UK aims to lead the G7 in AI adoption, but achieving this will depend on establishing a clear and supportive framework for innovation. If the UK gets this right, it has the opportunity to lead globally by building a system where AI development is powered by licensed, traceable creative input, rather than unregulated scraping." ■



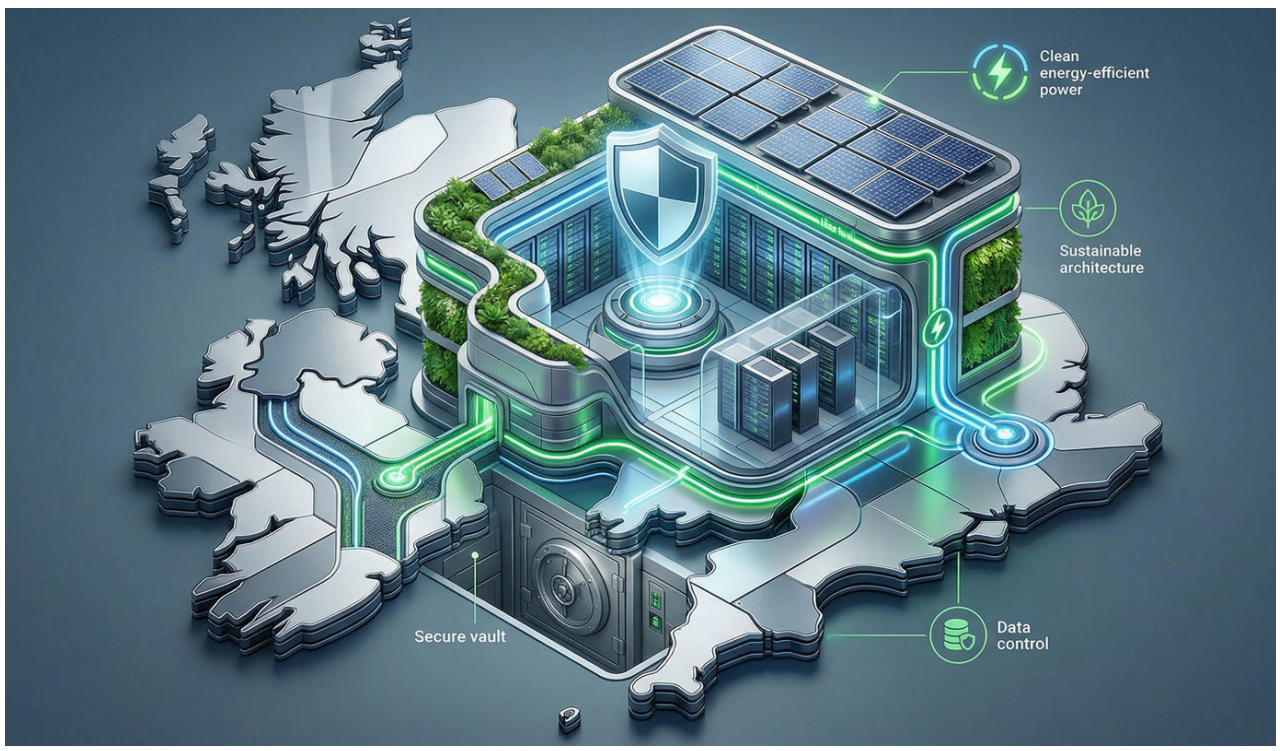
Push for energy efficiency

As the UK accelerates efforts to build out its AI infrastructure, new research from Argyll Data Development reveals that British businesses are increasingly demanding sovereign, energy-efficient AI platforms as a condition for adoption.

The research shows that sovereignty-compliant AI could significantly accelerate enterprise uptake. Some 64% of respondents said they would be more likely to adopt an AI platform if it met sovereignty requirements. This points to sovereignty not as a regulatory burden, but as a commercial enabler, particularly for organisations operating in regulated or data-sensitive sectors.

However, confidence in the UK's ability to support its long-term AI ambitions is mixed. Almost four in ten businesses (38.9%) believe the country lacks sufficient domestic compute capacity, with 32.8% saying the shortfall is already creating risk.

The findings underline the strategic importance of building resilient, home-grown AI infrastructure to avoid over-reliance on foreign providers. For many organisations, how AI systems are operated matters as much as what they do. More than seven in ten respondents said it is important that critical AI infrastructure is hosted within their own country or region. This reflects rising awareness of geopolitical risk, regulatory exposure, and the need for greater control over data and AI systems.



Alongside sovereignty, energy efficiency is becoming a core consideration for AI strategies. While performance remains critical, 51.2% of organisations said energy efficiency is important.

External pressure is also mounting. More than half of respondents said customers or stakeholders already expect organisations to address the energy usage of AI systems, including 21.0% who said it is an expectation from many stakeholders. A further 28.6% believe energy concerns will become an issue in the future, signalling growing scrutiny ahead.

"The message from UK businesses is clear: AI adoption will scale fastest when it is sovereign, efficient and sustainable," said Peter Griffiths, chairman, Argyll Data Development. "As the UK builds out its AI infrastructure, organisations are looking for solutions that deliver high-performance AI without sacrificing control, compliance or energy responsibility.

"Sovereign, energy-efficient AI isn't about slowing innovation – it's about making AI viable at national and enterprise scale. The organisations that get this right will be the ones best positioned to turn AI ambition into long-term value." ■

Passing the password test

One of the most persistent and underestimated cybersecurity risks is near-identical password re-use – a practice of adding or changing a character in an existing password, instead of creating a unique password. However, this practice can prove costly…

A new analysis reveals that a common habit of making small tweaks to existing passwords – such as adding a number or changing a symbol in an existing password, instead of creating a unique one – is a massive security risk that hackers easily exploit. Despite company policies and security training, this widespread practice of using near-identical passwords remains one of the biggest, most underestimated threats, cybersecurity experts warn.

This risky behaviour is indeed widespread. NordPass' password reuse survey reveals that 60% of Brits, 62% of Americans and 50% of Germans re-use passwords across multiple online accounts. On average, people re-use passwords for about five accounts, with one-fifth admitting to reusing them for 10 or more accounts.

"This risky habit, affecting nearly three in five users, creates a domino effect of vulnerability, where a single compromised password can unlock an entire digital life," said Karolis Arbaciauskas, head of product, NordPass.

Adding a letter, a number or a symbol

According to the survey data, 68% of Americans who re-use passwords make at least some changes before reusing them. The same is true for 62% of Brits and 61% of Germans. The most common change is adding or changing a number, symbol, or letter.

"Such a lax approach to security can result in stolen data or an emptied bank account, and a lot of anxiety," said Arbaciauskas. "However, I must agree that, in terms of sheer damage that a threat actor could do, this practice is an especially dangerous phenomenon in the corporate environment. Because it technically does not violate most password policies, and it often stays unnoticed by administrators. This way, it can become an entry point for threat actors, who would gladly extort or blackmail the company."

Most common variations

In the 'Top 200 most common passwords 2025' list, researchers found 119 nearly identical passwords, which were divided into seven approximate groups:

- Sequential number variations. Examples: 12345, 123456, 1234567,987654321.
- 'Admin' variations. Examples: admin, Admin, adminadmin, admin123.
- 'Password' variations. Example: password, Password1, p@ssw0rd, Passw0rd.
- Keyboard pattern variations. Examples: qwerty, qwerty123, abcd1234, Abcd@1234.
- Repetitive pattern variations. Examples: 11111111, 111111111, aa112233, aabb1122.
- Common word variations. Examples: welcome, Welcome1, test123, Test@123.
- Prefix/suffix variations. Examples: a123456, Aa123456, Aa@123456, 12345678a.

The most numerous groups are sequential number variations, keyboard pattern variations and repetitive pattern variations.

Arbaciauskas said: "This is just a rough breakdown, based on variations of the same passwords. However, in principle, all 200 passwords can be placed into certain predictable categories. For example, when compiling the list itself, we noticed that popular names and surnames, place names, swear words, brand names and equivalents of the word 'password' in various languages, are often used as passwords. Often with added numbers or special characters. Those passwords feel unique but are all predictable patterns. Threat actors know this, and the automated hacking tools they use, most certainly can apply common transformations, such as adding or changing characters and incrementing numbers."

Why do people re-use passwords?

A third of internet users who reuse passwords say they do it because they have too many accounts to manage different passwords for each one. About 25% say that they find it inconvenient to create and manage unique passwords.

Arbaciauskas continued: "People re-use passwords because it's easier that way. Between work tools, financial apps, subscriptions, social networks, online shopping and gaming, the number of accounts adds up quickly. The average person has around 170 passwords. Remembering unique passwords for all of them isn't realistic. However, it is worrying that, despite repeated warnings, about 10% of respondents still don't think there's a significant risk in re-using passwords. This mindset is a disaster waiting to happen. Threat actors could gain access to all your accounts, your identity could be stolen and your credit card – maxed out, or a loan could be taken out in your name. In a corporate setting, this behaviour could cost millions, if you let ransomware in."

Password safety tips

According to Arbaciauskas, a few general rules can greatly improve digital hygiene and help avoid falling victim to cyberattacks due to ineffective password management:

- Security training. Many companies are already doing this. Although this doesn't always work – sometimes even cybersecurity professionals get fooled – training bears fruit. Companies that run regular security workshops experience fewer cases of re-used credentials, and employees often use this knowledge in personal life.
- Password policies and technologies. Companies should have robust password policies. Ideally, the company's system would automatically compare newly created passwords with those already leaked on the dark web and prevent the creation of one that is the same or very similar to the one already leaked. It's best to use password generators for both personal and work accounts.
- Multi-factor authentication (MFA). So far, this is the most reliable and convenient way to provide additional protection for business and personal accounts. MFA, which requires you to provide a one-time code when logging in, can stop account takeover even when the threat actors have your password.
- Password manager. It can help you generate, store, manage, and safely share passwords. A password manager removes the need to rely on memory altogether. Instead of trying to come up with something clever or easy to remember it creates long, random passwords that don't follow patterns. And you don't need to remember them – just autofill or copy paste.
- Consider passkeys. A passkey pairs public key cryptography with device biometrics, so there's nothing to type, nothing to forget, and nothing to reuse. Although adoption is somewhat slower than expected, many major platforms already support them. Where passkeys are unavailable, turn on MFA. ■

Karolis Arbaciauskas: "People re-use passwords because it's easier that way."