

Future-proofing
the network

Overlaying SD-WAN
and WAN acceleration

David Trossell,
Bridgeworks, p5



Is liquid cooling
sustainable?

When planning the future, we
must think long-term

Paul Mellon,
Stellium Datacenters, p7



Questions
and answers

My hero was the original
Inspector Gadget

Jason Legget,
Connexin, p18



Co-op and M&S taken out by
DragonForce Ransomware-as-a-Service



Since Easter, two major UK retailers have been targeted by severe cyber-attacks. On 25 April, Marks and Spencer (M&S) was hit, followed by Co-op on 2 May. Several sources report that ransomware-as-a-service (RaaS) group DragonForce has claimed responsibility.

The consequences were devastating, impacting both finances and reputation. Hackers gained access to substantial amounts of customers’ personal data. M&S responded by suspending online orders, incurring a loss of approximately £3.8 million per day, and both retailers faced difficulties in restocking shelves. However, their immediate responses led to markedly different outcomes.

“While M&S experienced a major outage that has persisted for several days, Co-op appears to have detected the threat early and proactively shut down parts of its systems to prevent further damage,” notes Richard May, product development director (formerly CEO) of virtualDCS.

In response, the UK government has announced new cybersecurity initiatives aimed at strengthening retail sector defenses. These include a £16 million support package and increased funding for the CHERI project, which focuses on enhancing hardware security against cyber threats. Additionally, a

proposed regulation may prohibit public sector bodies and critical national infrastructure (CNI) organizations from making ransom payments under any circumstances, to reduce criminal profitability.

Industry experts emphasize that only a comprehensive approach — combining advanced technology, clear processes, ongoing vigilance, and public awareness — will enable businesses and consumers to navigate the evolving threat landscape.

“With increased public scrutiny on data protection and cybersecurity readiness, companies that neglect proactive measures risk significant financial losses and long-term damage to trust,” says Jake Moore, Global Cybersecurity Advisor at ESET. “Investing in expert-managed solutions, robust threat detection, and staff training can greatly mitigate operational and financial risks. However, cybersecurity is a collective effort — collaboration between the private sector, government, and experts is essential to safeguarding the UK’s digital economy.”

May adds, “immutable backups are vital for recovery, ensuring that clean data remains untouched by attackers. But their effectiveness depends on regular testing and integration into a well-rehearsed incident response plan. Combining strong monitoring, immutable

backups, and layered defense strategies will better prepare organizations for, and enable swift recovery from, cyberattacks.”

Meanwhile, Scott Dawson, CEO of DECTA, warns that this incident highlights how brittle legacy architectures and siloed security practices are, and no match for sophisticated threat actors.

“Until businesses adopt uniform metrics and invest in fail-safe recovery plans, every transaction — and every customer relationship — remains at risk,” highlights Dawson. “When a single intrusion forces entire back-office operations offline, every step from inventory management to customer service teeters on collapse. Businesses must move from reactive patchwork to proactive resilience engineering architected into every layer of IT strategy, or retailers will continue to pay the price. Only then can retailers protect revenue streams, reputations and the trust of the millions who rely on them.”

“The big takeaway from these incidents is that even well-resourced and established organisations are being tested by the speed and sophistication of today’s ever-evolving threat landscape. Recognising cyber risk as a business risk and investing accordingly must be a shared priority for all industries responsible for sensitive data,” asserts Kev Eley, Vice President UKI at Exabeam. ■

Cyber threats evolve.
Your protection should too.

Start with expert penetration testing

from
wavenet
cyberguard

Request a Quote >



Ofcom preparing to expand regulatory scope to include data centres in UK first

The UK government is planning to extend Ofcom's regulatory authority to include data centres, as part of efforts to enhance national cyber security under the upcoming Cyber Security and Resilience Bill (CSRB).

During a session with the Science, Innovation and Technology Committee on 20 May, Ofcom CEO Dame Melanie Dawes and Network and Communications Group Director Natalie Black discussed the evolving threat landscape and Ofcom's role in safeguarding critical infrastructure.

Black emphasized the importance of secure infrastructure design from the outset, staff training, and managing risks associated with third-party suppliers. She noted that while existing legislation already addresses some security concerns, the CSRB offers an opportunity to further strengthen protections and adapt to emerging threats.

Dame Melanie Dawes confirmed that the bill's scope will include regulation of data centres, which are now designated as critical national infrastructure (CNI). Ofcom has expressed willingness to regulate the sector more actively, with Minister Chris Bryant having approached the agency about expanding its oversight.

Under the proposed regulations, data centres with a capacity of 1MW or more would be in scope, while enterprise data centres exceeding 10MW would also be covered. The aim is to promote secure growth, investment, and resilience within the sector amidst an increasingly hostile cyber environment.

The government views this move as vital for levelling protections across utilities and ensuring that the UK's digital infrastructure remains resilient against cyber threats. Further details are expected to emerge as the legislation develops. ■

EE and Ontix deploy 80 small cells across Westminster

EE and Ontix have completed the installation of 80 small cells across Westminster, marking a major milestone in next-generation mobile infrastructure. Supporting both 4G and 5G networks, these small cells aim to improve reliability and high-speed connectivity in some of London's busiest areas.

This collaborative project with Westminster City Council demonstrates a strong commitment to advancing digital infrastructure. Designed specifically for lamppost deployment, the small cells prioritize safety and weight considerations, offering concentrated coverage to meet high demand while seamlessly integrating into the urban landscape. The equipment is painted to blend with street furniture, minimizing visual impact and reducing clutter by utilizing existing structures.

Ontix employed a comprehensive pre-staging process, including thorough testing and location preparation, to ensure optimal performance from day one. This proactive approach reduces deployment time and minimizes disruption in high-traffic zones, which is critical in Westminster's dense environment.

Following a standardized build process, the deployment ensures consistency across all sites, facilitating future expansion and upgrades. This innovative approach sets a new benchmark for small cell deployment, supporting more efficient network enhancements and maintaining Westminster's position at the forefront of mobile connectivity innovation.

"This small cell deployment showcases Ontix's expertise in small cell technology and our ability to deliver cutting-edge solutions in complex urban environments," said Jamie Olejnik, Head of Delivery Operations at Ontix. "Our latest deployment is a testament to our commitment to innovation, designed specifically for seamless integration into existing street furniture while delivering exceptional performance. The holistic approach reflects a commitment to balancing technological advancement with urban aesthetics, ensuring that all

stakeholders - from local authorities to end-users - are satisfied with the outcome."

"A modern city is powered by wireless broadband yet too often our residents and visitors struggle to get a signal, especially after dark. I'm proud we're working with Ontix and EE to improve connectivity for all those who visit, work or live in Westminster with the latest mobile communications technology," said Cllr Geoff Barraclough, Westminster City Council Cabinet Member for Planning and Economic Development.

"This innovative small cell deployment with Ontix enhances 4G and 5G mobile connectivity for EE customers across the City of Westminster, one of London's busiest areas serving not only as the centre of UK government but also a focal point for tourism and business. This project is the latest milestone in our network densification efforts as we continue to boost mobile capacity where it's needed most across the UK," said James Hope, Director of Mobile Radio Access Networks at EE. ■



South Western Railway launches high-speed Rail-5G WiFi

After several delays, South Western Railway (SWR) has announced that its new rail-side 5G mast network is now operational along a 70km stretch of its Main Line into London, between Basingstoke and Earlsfield.

This innovative 'Rail-5G' solution, supported by FirstGroup's rail division, involves track-side 5G mobile masts designed to deliver superfast onboard WiFi.

Initially planned for early 2023, the deployment took longer but now offers internet speeds reportedly up to 20 times faster than the previous average, making SWR the first train operator in Europe to introduce rail-5G WiFi. While other operators have used similar solutions, SWR's upgraded network aims to significantly improve connectivity, especially compared to earlier flaky onboard WiFi.

The company previously trailed a version of this technology on the Isle of Wight, achieving consistent broadband speeds of up to 1Gbps on a moving train. The current multi-gigabit network is described as delivering multi-gigabit internet capacity, enhancing the onboard experience for passengers.

Peter Williams, SWR's Customer and Commercial Director, emphasized the benefits: passengers can stream, download, video call, and work seamlessly, making train travel more productive and enjoyable. SWR also highlighted survey results showing that 41% of UK adults would be more likely to choose train travel if onboard WiFi was fast and reliable — rising to 64% among 16-24-year-olds — underscoring the importance of quality connectivity in boosting rail's appeal. ■



Cyberattack on NHS trusts raises concerns over patient data security, says NSCS

Recent cyberattacks have compromised NHS trusts, including University College London Hospitals and University Hospital Southampton, with experts warning that sensitive patient data may be at risk. The UK's National Cybersecurity Centre (NCSC) is actively monitoring the situation.

Analysis by EclecticIQ revealed that the breach occurred through exploitation of a software vulnerability in Ivanti Endpoint Manager Mobile (EPMM), a tool used for managing employee mobile devices. The vulnerability, first discovered on 15 May, has since been patched, but systems previously affected may still be vulnerable.

Rather than a ransomware attack, hackers clandestinely accessed data by

exploiting this software flaw, enabling them to explore systems and run programs remotely — a technique known as remote code execution (RCE). The data accessed reportedly included staff phone numbers, IMEI numbers, and authentication tokens, which could potentially lead to further breaches, including access to patient records.

EclecticIQ identified the hackers operating from an IP address in China, employing automated scans to find vulnerable systems rather than targeted attacks. The incident underscores ongoing risks to healthcare data security and highlights the importance of rapid vulnerability management in critical sectors. ■

EDITORIAL:

Editor: Amy Saunders

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Joe Potten, David Trossell, Jim McGann, Paul Mellon, Seva Vayner, Iwona Zalewska, Anthony Senter, Toby Sturridge, Jason Leggett

ADVERTISING & PRODUCTION:

Sales: Kathy Moynihan

kathym@kadiumpublishing.com

Production: Karen Bailey

karenb@kadiumpublishing.com

Publishing director:

Kathy Moynihan

kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Image Court, IC113, 328/334
Molesey Road, Hersham, Surrey, KT12 3LT
Tel: +44 (0) 1932 886 537

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

ISSN: 2052-7373

Eclipse Power Networks secures major contract with Colt Data Centre Services to develop hyperscale data centre campus grid connections

Eclipse Power Networks has announced a significant contract with Colt Data Centre Services to develop and maintain grid connections totalling 250MW for its hyperscale data centre campus in Hayes, Middlesex. This contract follows a competitive tender process that began in late 2023 and concluded at the end of 2024, with Eclipse providing ongoing support throughout.

Under the agreement, Eclipse will adopt a 132kV dual-circuit connection from National Grid's Uxbridge Moor substation, supplying 100 MW to the campus. Additionally, a 66kV dual-circuit connection from National Grid's

North Hyde substation will deliver a further 150MW. These connections will serve the campus's five data halls, each independently metered via Eclipse's network at 11kV.

"This critical infrastructure project highlights our technical expertise and ability to develop innovative, cost-effective solutions for mission-critical applications. Our collaborative and transparent approach helped Colt develop a unique commercial model that offers an innovative and equitable solution never before seen in Great Britain," said David Swadling, Group Sales Director at Eclipse Power. "By owning and

managing the grid infrastructure on Colt's behalf, we ensure reliable power for the facility while allowing Colt to focus on delivering sustainable hyperscale data centre solutions."

Eclipse's selection was driven by its extensive experience with extra-high voltage (EHV) networks, deep understanding of National Grid processes, and a commitment to stakeholder transparency to optimize the commercial relationship.

"As the UK advances in the global digital economy, our Hayes campus requires scalable, secure power solutions with expansion potential. Colt partners

only with organizations that share our commitment to mission-critical infrastructure. Eclipse's innovative, collaborative approach and expertise in power networking make them the ideal partner for our growth at Hayes," said David Knox, Global Director of Energy & Sustainability at Colt Data Centre Services.

With five floors and 175MW of IT capacity, Colt's Hayes campus represents a major investment in data centre infrastructure. Energisation is scheduled for 2028, with Eclipse Power Networks designing infrastructure to last at least forty years. ■

UK SMEs could unlock up to £78.1 billion in value by embracing AI


A new report suggests that UK small and medium-sized enterprises (SMEs) have the potential to generate up to £78.1 billion in economic value through greater adoption of artificial intelligence (AI). Despite widespread awareness of AI's benefits, many SMEs face significant barriers to implementation, including skills gaps, lack of clear guidance, and concerns over costs.

The study, commissioned by Microsoft and WPI Strategy, highlights an AI readiness gap among UK SMEs — 55% recognize AI's potential benefits, yet 46% admit to lacking the necessary expertise or understanding. Without targeted support and investment, many risk falling behind competitors already leveraging AI to improve decision-making, customer service, and operational efficiency.

Industry voices emphasize AI's critical role in enhancing customer experience, especially during economic uncertainty. Zoe Kelleher of AND Digital noted that AI can deliver smarter personalization and predictive insights, helping businesses retain customers and build loyalty amid turbulence.


The report calls for policy initiatives to improve AI accessibility and literacy among small businesses, including clearer pathways to adoption, affordable tools, and sector-specific awareness campaigns. Stuart Harvey of Datactics stressed that high-quality data is essential for AI success — fragmented or poor data can limit impact, making data governance a strategic priority.

Given that SMEs constitute over 99% of UK businesses and employ more than half the workforce, unlocking AI's full potential is vital for sustainable growth and global competitiveness. Industry experts urge immediate action from SMEs and policymakers to convert awareness into tangible results, ensuring the UK's economy remains future-ready. ■




MISSION: POSSIBLE

SECURING THE EDGE



CYBERSCOPE®

**EDGE NETWORK
ANALYZER
& VULNERABILITY
SCANNER**



**SEE US AT
INFOSECURITY EUROPE
STAND G146**

10 steps to better protect your business

The recent attacks on the retail sector aren't isolated incidents; Wavenet recommends 10 proactive measures to reduce your risk:

1. Deploy phishing-resistant multi-factor authentication (MFA)

Secure your access points with advanced MFA solutions including hardware security keys and modern app-based number matching.

2. Enforce strict call-back verification for password resets

Enhance your password reset procedures and instate strict call-back verification protocols. This ensures the identity is thoroughly confirmed before any sensitive account changes are made.

3. Implement network segmentation

Implement VLANs, firewalls, and access controls, and regularly test segmentation effectiveness to isolate critical systems and limit lateral movement by attackers.

4. Patch business-critical systems in a timely manner

Stay updated, monitor for new vulnerabilities, schedule and deploy patches, and verify successful updates to minimise the window of exposure to known exploits.

5. Regularly test your data backups, failover and failback

Schedule and conduct regular backup tests, including failover and failback exercises, to ensure data can be restored quickly and reliably in a crisis.

6. Monitor security logs for suspicious activity

Implement 24/7 security monitoring with a SOC, using advanced SIEM tools to manage suspicious activity in real time.

7. Perform regular penetration tests including social engineering assessments

Engage in regular CHECK and CREST-accredited penetration testing for technical and social engineering assessments, detailed reports and actionable recommendations to address weaknesses.

8. Create and rehearse business continuity & incident response plans

Regularly rehearse Business Continuity and Incident Response Plans and facilitate tabletop exercises and live simulations to ensure your team is prepared.

9. Prepare and protect your data using the 3-2-1 strategy

Regularly review backup strategies to ensure compliance and resilience, using the 3-2-1 rule: three copies of your data, on two different types of storage, with one copy off-site (or in the cloud).

10. Ensure your data is immutable or air-gapped

Configure immutable backups and set up air-gapped storage solutions, for maximum protection against ransomware and insider threats. Is your organisation prepared for evolving threats?

Your business must evolve too, and we can help: wavenet.co.uk/cyber

Three UK completes landmark OpenRAN trial

Three UK has successfully concluded one of the UK's first trials of OpenRAN (O-RAN) technology in a dense urban environment, specifically in Glasgow.

The trial, part of the SCONDA project supported by the UK government's DSIT, demonstrated impressive results, with peak 4G and 5G data speeds doubling — reaching up to 520Mbps for 5G.

The trial involved deploying compact O-RAN small cells on street furniture such as streetlights and CCTV poles to test the feasibility of urban deployment, which has traditionally been limited to rural or suburban areas. The move aims to increase vendor diversity, interoperability, and cost-efficiency by standardizing radio access network components.

"This is the UK's first Open RAN trial in a dense city environment, addressing unique technical challenges like legacy system integration and security, while delivering real improvements for customers. The encouraging results lay a strong foundation for expanding Open RAN deployment across urban areas," said Iain Milligan, Chief Network Officer at Three UK.

Following the successful testing at 18 sites, the project will now expand to 34 Open RAN small cell sites across Glasgow city centre, marking a major milestone for OpenRAN technology in the UK. ■

UK progresses on rural 4G network expansion via SRN Initiative

The UK Department for Science, Innovation and Technology (DSIT) announced that 50 government-funded rural 4G mast upgrades are now live across England, Wales, and Scotland, with 50 more planned by March 2026.

This is part of the £1 billion Shared Rural Network (SRN) project, a partnership supported by £501 million public funding and £532 million private investment, aiming to extend 4G coverage to 95% of the UK by end-2025.

The project involves sharing existing masts and constructing new ones, with significant work focusing on upgrading Emergency Services Network (ESN) masts to support all mobile operators and improve emergency call connectivity. Key areas benefitting include parts of rural England, Wales, and Scotland, such as the Berwyn Mountains, Brecon Beacons, and regions across Scotland and Wales.

Since the SRN's launch in March 2020, over 10,000 sq km have gained 4G coverage for the first time, with nearly 35,000 sq km now covered by all four UK networks (O2, Vodafone, Three UK, EE). Wales has seen notable improvements, with remote areas now covered by all four networks, sometimes requiring multiple masts for full coverage. ■

Jersey begins rollout of £80 million 5G network

Jersey Telecom (JT), supported by Ericsson, has announced the commencement of its approximately £80 million project to deploy a new 5G mobile network across the island.

After nearly two years of planning, trials, and pilots, the first phase is now live in Area 1 (St Ouen), marking a significant milestone in the island's digital infrastructure upgrade.

The rollout involves replacing the existing 3G network and upgrading the current 4G infrastructure, which is based on ZTE equipment now reportedly deemed a security risk by the UK government and others. Early testing indicates substantial improvements in signal strength, coverage, and download speeds.

The phased deployment will continue over several months, with full 5G Standalone (SA) service expected by the end of 2025, providing end-to-end 5G connectivity without

reliance on 4G networks. The rollout plan includes specific regional targets from May through November, with key areas such as St John, Trinity, St Martin, and Jersey's town centre scheduled for phased launches.

Additionally, JT has invested in core network upgrades in Guernsey, prepared to extend the new 5G capabilities once spectrum licensing is established by regulators.

JT CEO Daragh McDermott emphasized the company's commitment to continuous innovation and future-ready networks, while Deputy Lyndon Farnham highlighted the benefits of enhanced service, security, and resilience for residents and businesses.

Once completed, Jersey's 5G network will complement the island's full-fibre broadband infrastructure and will be among the few globally to feature end-to-end Ericsson 5G technology. ■

Local opposition grows against Google's proposed data centre at North Weald Airfield

Google has applied for planning permission to develop a large data centre on a 52-acre site at North Weald Airfield in Essex, following its purchase of the land for approximately £1.7 million per acre (£88.4 million total).

The proposed development includes two data centre buildings, offices, and an on-site substation, totalling over 830,000 sq ft of floorspace, while the existing airfield operations are set to continue.

However, the local North Weald Bassett Parish Council has formally objected to the plans. Concerns include potential noise, glare from solar panels, and the impact on airfield operations. The council also raised issues about safety and security risks associated with a proposed viewing bund outside the secure perimeter, and the potential threat to the character and setting of the Grade II-listed Air Control Tower, which they say could be diminished or compromised.

The parish council criticized the application for lacking clarity on how security, safety, and operational impacts on the historic airfield would

be managed, and noted that alternative designs to preserve views and protect heritage features had not been sufficiently explored.

A Google spokesperson stated that the project aims to support the company's growth and enhance the UK's digital infrastructure, describing the development as a strategic move to ensure future technical expansion.

Historically, North Weald Airfield has a rich military history, dating back to World War I and World War II, serving as a Royal Flying Corps aerodrome and later as an air force base. Today, it functions as a commercial airfield for private pilots, training, and emergency services.

Local officials had previously expressed optimism about the land sale's potential to boost the economy and create jobs, highlighting the strategic importance of the site's development. However, opposition from the parish council indicates ongoing tensions between heritage, safety, and development interests. ■

Word on the web...

Is emerald steel the answer for UK DCs?

Joe Potten, Team Lead,
BCS Consultancy

To read this and other opinions from
industry luminaries,

visit www.networkingplus.co.uk



Paul Colwell,
CISO, Wavenet





Overlaying SD-WAN and WAN acceleration for a future-proof network infrastructure

David Trossell, CEO and CTO, Bridgeworks

With advancements in AI/ML, cybersecurity threats are becoming increasingly complex and persistent.

Jane Frankland, CEO of KnewStart, writes in her 'Key Cybersecurity Trends for 2025. My Predictions' blog that "an attacker could map a country's power grid vulnerabilities without triggering any alarms, setting the stage for future, large-scale operations."

She also predicts that cyber-crime will cost \$12 trillion in 2025. Ransomware remains the main threat, but how it's unleashed is evolving.

"Additionally, the use of customisable ransomware-as-a-service (RaaS) platforms is now mainstream, enabling even novice threat actors to launch professional-level attacks. With 24% of all data breaches using ransomware, this commoditisation of cybercrime significantly broadens the field, resulting in a sharp increase in the frequency and variety of attacks," adds Frankland.

To obfuscate cyber-criminals, greater investment in cyber-security is needed.

Times-are-a-changing

Traditionally, the answer to securely transmitting data, backing it up and restoring it, has been WAN Optimisation, which, unfortunately, often doesn't live up to its promise. For example, it can't transmit and receive encrypted data.

Next in line are SD-WANs - a great technology - but they often could do with a WAN Acceleration boost. There's also Secure Access Service Edge (SASE), which often incorporates SD-WANs and security functionalities to securely connect users and resources regardless of location.

Gartner finds that SASE is rapidly gaining in popularity - predicting that the market for SASE will reach over \$25 billion by 2027. It is also thought that in 2024, 40% of enterprises will have explicit strategies to adopt it. SASE adoption is expected to continue to grow in 2025, as it's widely thought that many enterprises are planning to implement it, or they are already doing so.

This upsurge is driven by a requirement need for secure, efficient access to cloud applications and resources in hybrid environments. Still, SD-WANs - next to WAN Optimisation - are still more popular. Yet, SASE - perhaps because it also includes SD-WANs - is expected to take the lead. Yet, they often don't adequately deal with the network Gremlins of latency and packet loss.

Creating synergy

Nevertheless, WAN Acceleration with technologies offer synergy with SD-WANs. With AI, ML and data parallelisation, WAN Acceleration mitigates latency and packet loss, while enabling organisations to utilise 98% of their network's bandwidth without having to invest in new network infrastructure. When overlayed onto SD-WANs, it provides a boost in network performance, including for backups and restores to ensure regulatory compliance and to maintain service continuity in the face of cyber-attacks.

Not only does WAN Acceleration help to protect data in flight and create a robust and future-proof network infrastructure, it can be used to improve the performance and security of cloud-based applications, which are often impacted by latency and packet loss. A slow network connection can render cloud applications useless, and an insecure connection can create data security risks.

SD-WANs and WAN Acceleration therefore

complement each other with SD-WANs, providing intelligent routing and traffic management. Meanwhile, WAN Acceleration enhances data transfer speeds, data security in flight and efficiency by mitigating latency and packet loss. To achieve this ideal partnership, WAN Acceleration must be overlayed onto SD-WANs.

Backing up and restoring data

SD-WANs and WAN Acceleration together offer a means to improve the performance of backing up and restoring data, as well

as of cloud-based applications - helping organisations to achieve and maintain compliance with regulatory frameworks, such as HIPPA and GDPR. However, they are just part of the cybersecurity solution because organisations should always locate their data centres and disaster recovery sites outside of their own circles of disruption, and back up data in at least three separate locations.

The problem is that distance often increases latency, and there aren't alternative solutions on the market today that can mitigate latency as well as WAN Acceleration, which is not WAN Optimisation - despite the

claims. It renders concerns about distance obsolete, and it enhances SD-WANs. However, due to the physics of latency, it can only be mitigated, not eliminated completely. Yet, they go a long way to reduce its impact.

Enterprises should therefore explore adopting an SD-WAN-WAN Acceleration overlay strategy as part of their bid to obfuscate cyber-criminals, and to improve their ability to back up and restore data to maintain operations when disaster strikes - not mention the benefits of better cloud-application performance, more accurate big data analysis, and team collaboration. ■

MobileMark

antenna solutions

STAY CONNECTED

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

www.MobileMark.com

Contact Us Now:

+44 1543 459555

enquiries@MobileMarkEurope.co.uk



Shadow encryption: a new chapter in ransomware's evolution



**Jim McGann, CMO,
Index Engines**

Ransomware has come a long way from its early days. What began as random attacks on data centres has transformed into a high-stakes game of cat and mouse. The latest tactic raising concern among security professionals is known as shadow encryption, a kind of stealthy and sophisticated method designed to evade traditional detection and force organizations into paying massive ransoms.

At the core of ransomware's evolution is one unchanging motive, profit. Threat actors are looking to make money and they're targeting million-dollar payouts. Many operate from regions where enforcement is lax or non-existent, and in some cases, with tacit or direct support from 'the state.'

Ransomware evolution

In the past, ransomware campaigns often relied on relatively simple malware strains. These would execute in an obvious and indiscriminate way, encrypting data and then immediately demanding payment. Older malware like Xorist or TimeTime were noisy, and their activity could be detected more easily, giving organizations a chance to recover through backup and disaster recovery systems.

As security tools improved, attackers

Hard to detect, hard to beat

Modern shadow encryption tactics now go beyond intermittent encryption or encoding tricks. Some are capable of encrypting files in memory rather than on disk, leaving fewer traces for forensic tools. Others apply multiple encryption algorithms in succession, complicating both detection and decryption. These layered methods further blur the lines between clean and compromised data.

The sophistication of these techniques means traditional data protection tools, especially those built around storage or backup detection, are increasingly outmatched. Many organizations find out too late that they've been attacked, only realizing the scope of the damage once access to critical data is lost.

What can be done?

The emergence of shadow encryption marks a turning point in how organizations need to think about ransomware defense. Legacy detection tools are no longer sufficient on their own. To keep up with evolving threats, businesses must adopt more intelligent, adaptive technologies.

Artificial intelligence and machine learning can play a critical role in spotting

"The emergence of shadow encryption marks a turning point in how organizations need to think about ransomware defense. Legacy detection tools are no longer sufficient on their own."

adapted. With access to better technology and growing financial rewards, ransomware authors began to develop more advanced techniques. This led to the emergence of shadow encryption, an approach that prioritizes stealth.

What is shadow encryption?

Shadow encryption refers to methods of encrypting data in ways that avoid triggering traditional security alarms. The tactic gained notoriety in 2021 with the appearance of LockFile, a ransomware variant linked to the Conti gang. LockFile introduced intermittent encryption, a technique that encrypts only portions of each file leaving large sections untouched. This keeps compression ratios and entropy levels within normal ranges, making the attack harder to detect through conventional anomaly-based tools.

But intermittent encryption was just the beginning. As ransomware groups realized the benefits of shadow techniques, they began to add in new strategies to quietly wreak havoc. One method was when Chaos ransomware began using Base64 encoding to conceal itself. By transforming binary data into ASCII format, Base64 makes malicious content less conspicuous to security filters, allowing it to bypass many standard detection systems.

subtle behavioural changes that signal shadow encryption in progress. Unlike traditional tools that rely on known patterns or signatures, AI systems can identify anomalies in how data is accessed, modified, or transmitted, even when those changes are too subtle for humans or some tools to detect.

Beyond AI, organizations should embrace a multi-layered security approach that includes real-time threat detection at the file and memory level, endpoint protection with behaviour analytics, immutable backups and secure, off-network storage and zero-trust frameworks to minimize the spread of malware.

Looking ahead

Shadow encryption isn't just a new trick, it's a shift in strategy. Ransomware is becoming more evasive, more intelligent, and more damaging. The financial and reputational risks for businesses are growing, and the cost of inaction is rising.

Staying ahead of ransomware now requires more than just reactive security. It demands a proactive approach, with next-gen tools, smarter analytics, and an understanding of how threats are changing. Shadow encryption is here, and it's only going to get more sophisticated. The question is whether organizations are ready to tackle it. ■

Independant UK Datacentres & Server Hosting

Who we support:

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



velox
serv

0800 084 3521

www.veloxserv.co.uk

Protect Monitor Control

AKCP

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



How hot is your Server Room?

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

Server Room®
environments

0800 030 6838

projects@serverroomenvironments.co.uk



Cooling



Power



Energy



Fire



Monitoring



Racks



Networking



Consultancy



Services



Is liquid cooling a sustainable, long-term solution for UK data centres?

Paul Mellon, Operations Director, Stellium Datacenters

The data centre community has spent the last ten years investing in air cooling systems for racks. These were mostly indirect air systems that could provide effective cooling for racks up to 20kW and deliver a very credible PUE of 1.2. These data centres were mostly purpose built for these deployments and did not require significant external footprint.

The seismic shift to AI/HPC has caused significant supply/demand issues not just in the UK but across Europe and the world in general. Going forward, data centres will be designed to accommodate AI HPC (Training model) for racks up to 150kW, AI HPC (inference model/edge) for racks up to 50kW and HPC cloud for racks up to 50kW. The migration of our existing data centre base in the UK to support these rack power densities will create many challenges.

Flexibility and efficiency

The most compelling selling points for liquid cooling are its flexibility and efficiency. As liquid cooling systems are closed loop their usage of water is negligible. Liquids transfer heat far better than air, meaning servers run cooler with less energy than just blowing air around.

The result? A lower Power Usage Effectiveness (PUE) and actual savings on electricity bills. Plus, higher-density racks (think GPU-packed clusters) are far easier to manage when you're circulating liquid directly over the hottest components instead of fighting heat pockets with airflow.

Liquid cooling of racks can be configured to match power densities from 20kW to 200kW and beyond. This form of cooling requires the least restructuring of the GPU's and supporting IT technology.

Location, location, location

Depending on the location of the data centre it may not require evaporative cooling which will demand significant water usage.

South of Birmingham evaporative cooling will most likely be required whereas the North of UK will most likely run without evaporative cooling. From a sustainable perspective there are KPIs around water (WUE) as well as power (PUE).

There are further carbon elements in the location of data centres. The Southeast UK being the highest at 309g CO2/kWhr compared with the North east UK at 25g CO2/

kWhr. When implemented correctly - location, design, monitoring and operation the environmental benefits can be substantial.

The higher 'waste' heat from a liquid-cooled system can be captured and reused more readily, making district heating projects a real possibility and a potentially lucrative energy-recycling strategy for operators.

The UK has set ambitious goals around cutting carbon emissions, with the Northeast of the UK around Newcastle currently having the lowest output. Data centre operators are under the microscope, and cooling is a big piece of the sustainability puzzle. Because liquid cooling can significantly reduce the power needed for thermal management, it's becoming increasingly attractive to businesses looking to burnish their green credentials.

There's also the question of resilience in a warming climate. The UK may be mild compared to some parts of the world, but summertime heatwaves and rising average temperatures mean air-cooled data centres often must crank up the fans to cope. Liquid cooling can be a more stable, predictable solution, regardless of seasonal fluctuations.

Installing liquid-cooling infrastructure can initially seem expensive, especially considering the need for specialised equipment and possible retrofitting at older data centres. However, the operational savings in energy often offset those costs

pay off later, both in monetary and sustainability terms.

Implementing liquid cooling can be more complex and expensive upfront. It often requires revamped infrastructure, specialised piping, and sometimes entirely new server

"The most compelling selling points for liquid cooling are its flexibility and efficiency. As liquid cooling systems are closed loop their usage of water is negligible. Liquids transfer heat far better than air, meaning servers run cooler with less energy than just blowing air around."

over the long run. As more hardware vendors adopt liquid-ready components, the investment hurdle is slowly decreasing.

Future-proofing

Let's also not forget the invaluable intangible: future-proofing. As workloads become more compute-intensive (AI, HPC), designing a data centre around higher densities will

designs. Retrofitting these systems in older data centres isn't always a trivial task.

For many UK data centres — especially newer facilities or those dealing with AI, machine learning, and HPC workloads like Stellium in Newcastle — the short answer to our title question is 'absolutely.' It's a robust, energy-efficient, and increasingly cost-effective way to tackle current and future thermal challenges. ■



CACI + **f5**

Upcoming webinar Taming API Chaos: Pain points and the F5 advantage

Uncover how to simplify, secure and scale your API ecosystem with CACI and F5.



Wednesday 25th June
11:00am - 12:00pm



www.info.caci.co.uk/taming-api-chaos





STULZ

CLIMATE.CUSTOMIZED.

YOUR COOLING EXPERT FOR THE FUTURE

YOUR PARTNER IN THE UK FOR
DATA CENTRE, IT & LIQUID COOLING





Network lockdown: cyber resilience rules for every business

In 2025, network security is a business-critical priority. The rising sophistication of cyber threats, tighter data protection regulations, and the explosion of connected devices have forced businesses of all sizes to rethink how they defend their digital perimeters.

From budget-stretched SMEs to global tech giants, the challenges are universal — but the strategies vary. We asked leading experts in network security to weigh in on what's working, what's affordable, and what every organisation needs to do to stay ahead of evolving cyber threats. Their responses paint a clear picture: security starts with visibility, is powered by smart design, and ultimately hinges on doing the basics — brilliantly.

Legislation with teeth

Few forces have reshaped the network security landscape more dramatically than the General Data Protection Regulation

(GDPR) and the UK Data Protection Act. Their influence goes far beyond compliance paperwork.

“UK regulations like the GDPR and the Data Protection Act enforce strict guidelines on how businesses collect, process, and store personal data,” explains Gerald Beuchelt, CISO at Acronis. “They require robust security measures such as encryption, regular risk assessments, and clear breach notification protocols to ensure compliance, regardless of business size.”

This shift has been particularly transformative for smaller companies that once assumed security was only a concern for the enterprise tier.

“Regulations like the Data Protection

Act and the upcoming Cyber Security and Resilience Bill have raised the stakes when it comes to protecting data,” says Gary Cox, Director of Technology for Western Europe at Infoblox. “For a lot of businesses, but particularly smaller enterprises with limited resources, complying with this kind of legislation can feel utterly daunting — but compliance doesn't have to mean a complete overhaul.”

Evan Davis, Senior Manager of Solutions Engineering at TRENDnet, adds: “the GDPR and Data Protection Act influences security measures heavily, but Cyber Essentials predates GDPR/DPA. While not required, it served as a guide for businesses as to the ‘appropriate measures’ outlined for cybersecurity.”



Jonathan Whitley, WatchGuard

For some, the regulatory landscape is even broader.

“There are also other rules and regulations to consider depending on your organisation’s industry,” warns Crystal Morin, Cybersecurity Strategist at Sysdig. “For financial companies doing business in Europe, for example, the Digital Operations Resilience Act (DORA) will likely apply.”

“Much of this has been done by a strong community of MSSP professionals who are providing ongoing services to their customers,” says Jonathan Whitley, Regional VP for Northern Europe at WatchGuard, noting that these frameworks can also open new business opportunities for those who achieve compliance.

Security on a shoestring

With tighter margins and leaner IT teams, particularly amid the present cost of living crisis, SMEs need to prioritise smart investments and strategic partnerships.

“Now, more than ever, businesses are finding themselves in a position where they have to do more with less, particularly when it comes to cybersecurity,” notes Cox. “But security doesn’t have to come with a huge price tag. For SMEs, cloud-managed services that combine DNS, DHCP, and IP address management (often referred to collectively as DDI) are a good starting point, particularly if real-time threat detection is included. These tools increase visibility, reduce complexity, automate monitoring and alerts, and provide early warnings of suspicious activity without the need for a large in-house security team.”

According to Morin, open-source security tools are the most cost-effective



security tools available for free,” advises Morin. “Consider using Open Policy Agent (OPA) to manage compliance with

“Now, more than ever, businesses are finding themselves in a position where they have to do more with less, particularly when it comes to cybersecurity. But security doesn’t have to come with a huge price tag. For SMEs, cloudmanaged services that combine DNS, DHCP, and IP address management (often referred to collectively as DDI) are a good starting point, particularly if real-time threat detection is included.”

solution for any organisation operating with a tight budget.

“And they don’t need to worry about missing out on adequate protection either, because there are some incredible

policy as code, making it easy to enforce policies across your entire environment. For real-time threat detection and the ability to start automating incident response, look at Falco. Using an open-source tool does mean that your organisation is the responsible maintainer for your deployment, and you must take care of patches and updates. But there are massive communities in place around open-source security projects like Falco that provide support.”

Beuchelt agrees that leveraging open-source tools, cloud-based security services, and affordable endpoint protection solutions can be effective: “the solution should integrate essential functionalities such as automated backup, disaster recovery (DR), patching and remote device management, and robust endpoint protection and response. These components ensure that you have comprehensive visibility into network activities and can generate detailed reports in the event of an incident.”

Looking into the hardware, Phil Huang, Business Development & Field Application Manager at D-Link,

suggests that SMEs should look to deploy enterprise-grade Wi-Fi 6 access points with the latest WPA3 Wi-Fi encryption for secure connectivity, and network management software, for centralised network management - all whilst reducing operational costs.

“Use a good router with a built-in SPI firewall and port blocking,” adds Davis. “For further protection, some routers feature IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems).”

Designing for defence: network architecture essentials

Simple, segmented, and secure — experts agree that a well-structured network is often the best deterrent.

“SMEs should design a simplified but segmented network architecture that isolates critical systems from less secure parts of the network,” says Beuchelt. “Key elements include strong identity governance, including robust multi-factor authentication (MFA) and strict password policies. This permits the adoption of a Zero Trust model — ideally with continuous verification.”

Morin, too, recommends segmenting the network and separating sensitive and proprietary data across the segments so that, in the event of a breach, the business can limit lateral movement and minimise the blast radius.

“Scan constantly and assess regularly. Like threat detection for active attacks, you should be constantly scanning your environment for vulnerabilities and remediating those that are in use in your production environments, have a known exploit available, and are of the highest severity,” adds Morin. “You’ll never be able to fix all vulnerabilities, so prioritising them properly is imperative. Also, you should conduct vulnerability

assessments and penetration testing on a regular basis, if possible, to identify potential weak points.”

Meanwhile, Huang reiterates that security and simplicity should be kept in mind.

“Using VLANs to segment traffic between different departments and guest access, enabling WPA3 encryption on the Wi-Fi network and strong endpoint protection can all contribute to a more secure network. Adding a firewall gateway with built-in Intrusion Prevention System, Dynamic Web Content Filtering and Application Control provides an extra layer of security to your network. Having a network that can be centrally managed through software or hardware controllers can help to simplify tasks such as firmware upgrades, Wi-Fi password changes, VLAN settings as well as an instant overview of the live usage and health of the network,” says Huang.

Indeed, controlling who can access what, and when, is foundational to network security — and often overlooked.



Phil Huang, D-Link



Evan Davis, TRENDnet

“Role-based user accounts, multi-factor authentication (MFA), and enforce strict policies designed around Zero Trust Architecture,” says Davis. “Minimise worker access to internet and network resources to only those needed for the job role.”

“Effective access control involves a combination of MFA, role-based access controls (RBAC), and periodic reviews of user privileges,” adds Beuchelt. “This ensures that sensitive data is only accessible to authorised personnel.”

Morin adds a tactical note: “take a look at your access requests. How many accounts haven’t been used in the last 30 days? How many granted accesses have authenticated users not used in the last 30 or 60 days? Unused accounts and excessive, unused permissions should be removed – otherwise, they are unnecessary risks that could be misused by an attacker. Review access regularly.”

Whitley asserts that identity security is a key underpinning of a good cybersecurity strategy. Ensuring that companies big and small start with the approach that preventing unauthorised users from accessing corporate resources is key.

“Many data breaches are as a result of accidents by people, or by well-meaning staff falling foul to a phishing attack. For this reason, ensuring that staff only have access to those resources they need help prevent accidental or malicious breaches, and where these breaches are not prevented, they will nevertheless mitigate the worst consequences,” notes Whitley.

Eyes on the horizon

Network threats aren’t standing still — and neither can we.

“The only thing we can be certain of is that threats continue to evolve. Unfortunately, the money made by bad actors mean they will have considerable resources to keep looking for ways around defences,” highlights Whitley. “For this reason, the key is to be constantly vigilant. Even when you think you have strong defences constantly monitor them and ensure your managed service provider is doing the same.”

Beuchelt believes that emerging trends such as AI-driven threat detection, Zero Trust architectures, and enhanced cloud security are shaping the future of network defense.

“Businesses, especially SMEs, should keep abreast of these technologies and continuously update their security strategies and staff training to stay ahead of evolving cyber threats,” notes Beuchelt.

Cox agrees that “AI-powered threat detection and Zero Trust security models are no longer just for the enterprise end of town. SMEs should take note – these technologies are becoming more accessible and can help spot and stop threats before they do damage, particularly when coupled with AI and real-time threat monitoring. DNS-based security plays a key role here, offering a lightweight but powerful way to enforce policies and gain deeper visibility into network activity. You can’t stop what you can’t see, and DNS provides the eyes and ears businesses need to increase their resilience and safeguard their perimeters.”

“AI and large language models (LLMs) are becoming more prevalent both in cyberattacks and security tools. Defenders

must be able to use AI-enabled security tools to expedite their workflows and defend against AI-powered attacks,” recommends Morin.


The overwhelming message from experts? Don’t wait.

“Don’t just take these steps now – do them consistently,” says Morin. “Regular security audits and employee training will foster a culture of security awareness.”

Whether you’re securing a single-office SME or a multi-site enterprise, the fundamentals are the same: visibility, segmentation, access control, and rapid response. As technology evolves and threats escalate, these pillars will be the foundation on which cyber resilience is built. ■




Crystal Morin, Sysdig




PILLER

Power Systems

Nothing protects quite like Piller



M+500




M+1200

M+ Series Static UPS is here

High-Density, Hot-Swappable Modular Power Protection,
from 250-1200 kW

Piller UK Ltd | uk@piller.com | +44 1285 657 721



A Langley Holdings Company



Gary Cox, Infoblox



Advancing UK public safety with connectivity and innovation

The future of the UK's critical communications networks lies in the adoption of new technologies offering increasing bandwidth, coverage, and interoperability...

The landscape of critical communications in the UK is evolving rapidly, driven by technological advancements and growing operational demands.

Simon Clifton, Head of Pre-sales at Simoco, highlights that while the UK's Airwave TETRA network provides secure and reliable voice communication across the country, other critical data and broadband users rely on public or private LTE services: "the challenges around this are to do with consistent network coverage and available bandwidth across relatively small distances, which often means calls or data streams are dropped whilst on the move."

This variability in coverage and bandwidth can hinder frontline responders during urgent situations. Experts agree that relying solely on traditional professional mobile radio (PMR) or commercial mobile services is outdated.

David Turner, General Manager at Tait Europe, emphasises that many nations are leveraging existing PMR networks and their core functionalities to bridge the gap to broadband: "presenting first responders with a binary choice of PMR or commercial mobile service is not right and quite naïve. Many countries and agencies are leveraging existing PMR networks and core functionality to bridge first responders to an existing broadband network by focusing on the core of the networks, as well as the associated system integration."

This approach allows for quick access to mission-critical voice alongside data applications, enhancing operational efficiency.

Transitioning from legacy to broadband

Although TETRA has served as the backbone of critical communications since the 1990s, its limitations are becoming increasingly apparent. Challenges such as low data bandwidth, spectrum constraints, limited device options, and compatibility issues with modern broadband technologies are prompting a shift.

"The change to broadband is driven by an increasing demand for higher data rates and enhanced multimedia communication," explains David Gibbs from Zebra Technologies.

Frontline teams now need to digitalise evidence, share real-time data, and communicate via voice, text, and video — all in high-pressure environments. Migration to broadband not only offers higher capacity and lower latency but also opens the door to advanced applications like AI, augmented reality, and real-time video, which can transform emergency response.

"With the right mobile computers, we could also hope to see useful AI and augmented reality applications for public safety professionals in the field," notes Gibbs. However, he warns that continued reliance on legacy TETRA networks may lead to increased costs, especially as older devices become harder to maintain and parts become scarce.

It's widely considered that the rollout of 5G brings promising features that could revolutionise mobile critical communications.

One key advancement is network slicing, as Gregor Tomic of Rohde & Schwarz explains: "5G network slicing will serve as a foundational element for future MCX-based services, providing a more robust and reliable framework for prioritising high-priority users."

By creating dedicated slices for emergency services, organizations can ensure high availability and low latency even in congested environments.

Demand for multimedia support — voice, data, and video — is also increasing. The deployment of hybrid devices that combine LTE and 5G ensures seamless mobility and backward compatibility, facilitating a smoother transition.

"The rollout speed of networks is influenced by cost, standards, and spectrum availability, with a trend toward adopting 3GPP LTE services for voice, data, and video support," says Gibbs. He also highlights that private 5G networks can significantly

support critical operations by enabling multiple simultaneous video streams and replacing costly legacy systems.

Prioritising data and managing bandwidth - effectively

Bandwidth management remains vital during emergencies, where every second counts.

Tomic underscores that ensuring high Quality of Service (QoS) is crucial: "the ability to transmit real-time video and other critical information in a reliable and timely manner is crucial for ensuring the safety and effectiveness of emergency response operations."

Strategies such as network slicing and application-layer prioritisation can segregate critical data from non-essential traffic, ensuring vital communications are maintained during peak loads.

Clifton adds, "bandwidth management is critical; there are two ways this can be achieved—either by making the entire network Mission Critical ready (MCx) or by slicing the available bandwidth to segregate a section for the critical communications only."

Proper planning and testing of these configurations are essential to prevent failures in high-stakes situations, since effective emergency response often depends on seamless communication across different agencies.

Turner stresses the importance of open platform interfaces: "an open platform interface can connect all the data services together, and then curate it based on what user organisations want and need."

This approach minimizes the need for device replacements and encourages system integration.

Gibbs notes that interoperability is essential for moving forward: "frontline teams need devices that can communicate with other LTE/broadband devices as well as TETRA devices. Different agencies will

progress at different paces, and there are regional variations in 5G rollout."

Ensuring flexible, multi-standard devices and systems helps maintain coordination during critical operations.

Embracing emerging technologies

The UK's critical communications landscape is on the cusp of transformative change, driven by 5G, broadband, and innovative network architectures. Experts agree that ensuring reliable coverage, prioritising bandwidth, fostering interoperability, and safeguarding security are vital for effective emergency response on the move.

Tomic highlights the potential of Non-Terrestrial Networks (NTN) and sidelink technologies: "NTN, which utilizes satellites and other platforms, can provide coverage where terrestrial networks are compromised — especially during catastrophic events."

Combining NTN with 5G sidelink enables direct device-to-device communication, essential in environments where infrastructure is damaged or overloaded.

Clifton envisions a future where multiple IP networks operate in parallel — private or public 4G/5G, Wi-Fi, satellite, and mesh networks — creating resilient, global coverage for voice and data.

"It is now possible to build a critical voice and data solution that will work in any place on Earth by using these networks together," asserts Clifton. Preparing for this technological convergence requires organizations to adapt their networks, upgrade infrastructure, and foster interoperability standards.

Entering a new era, powered by 5G, broadband, and satellite, the UK's critical communications systems are integrating diverse networks and ensuring robust coverage, better equipping responders with seamless operations — no matter the challenge. Adaptation and interoperability are key to building a resilient, future-proof communication landscape. ■



AI inference: the secret to smarter business

Seva Vayner, Product Director, Edge Cloud and Edge AI at Gcore

Artificial Intelligence (AI) is transforming how businesses operate, driving innovation in almost every industry. According to a 2024 survey by Writer, 89% of enterprises are either actively using or exploring AI solutions, with AI inference playing a crucial role in deployment. Additionally, the survey found that 47% of companies have already integrated AI into customer support functions, while 45% are using AI for business process automation.

This growing adoption of AI reflects its increasing importance in modern operations and decision-making. While much of the focus has historically been on AI model training, AI inference – the process of

the cloud. With this approach, inference workloads can operate efficiently, without being hindered by slow networks or high compute costs.

Overcoming AI scalability and cost challenges

One of the big hurdles businesses face is balancing the performance of AI systems with cost-efficiency. Traditional AI inference models often require powerful hardware, making them too expensive for widespread use. Businesses need to find ways to optimise AI processing without overloading their infrastructure or increasing costs too much.

“By integrating AI inference with edge computing, companies can spread workloads more effectively, reducing their reliance on centralised cloud resources. Modern solutions provide global edge infrastructure with numerous PoPs, enabling businesses to process AI tasks closer to their customers.”

applying trained models to real-world tasks – is now emerging as the key differentiator for companies looking to make the most of AI.

Whether it's providing real-time customer support or improving decision-making through predictive analytics, AI inference is changing how enterprises operate by offering faster insights and automation. But as businesses look to deploy AI inference effectively, there are still several challenges to overcome. Here, we explore five key factors that make AI inference so important for modern businesses.

The shift to real-time AI processing

AI-powered applications, including chatbots, fraud detection systems, and autonomous vehicles, require real-time processing to function smoothly. Traditional cloud setups can struggle with latency, which is where edge AI comes in. By running AI inference at the edge, closer to the data, businesses can reduce delays and improve responsiveness.

Sophisticated solutions today offer scalable, low-latency solution for AI applications, whether on-premises or in

By integrating AI inference with edge computing, companies can spread workloads more effectively, reducing their reliance on centralised cloud resources. Modern solutions provide global edge infrastructure with numerous points of presence (PoPs), enabling businesses to process AI tasks closer to their customers.

This reduces latency, enhances speed, and optimises costs by minimising reliance on centralised cloud resources.

Improving data security and compliance

As more businesses adopt AI, the need for strong data security and compliance grows. Industries like telecoms, finance, and healthcare have strict regulations that require AI workloads to be processed in secure environments.

Advanced AI inference solutions now allow businesses to deploy and monitor AI models within their own secure infrastructure while still benefiting from cloud scalability. This enables companies to leverage AI technologies without compromising compliance or exposing sensitive data to unnecessary risks.

The power of open-source and strategic partnerships

Collaborations and open-source technologies are playing an increasingly important role in the successful adoption of AI inference. Open-source frameworks simplify the deployment process, while strategic partnerships ensure businesses can access the latest innovations to stay ahead of the competition.

For example, Gcore partnered with Mirantis, combining Mirantis' expertise in cloud-native technologies with Gcore's edge AI capabilities. This collaboration will allow businesses to optimise their AI infrastructure,

simplifying deployments and improving performance. Partnerships like this are vital for addressing the growing demand for AI-driven applications and simplifying the complexities of infrastructure management.

The future of AI inference: Accessibility and automation

As AI technology evolves, the focus is shifting towards simplifying AI inference, making it easier for businesses to implement and manage. The next phase will see solutions that enable quicker, more efficient AI model deployment, without requiring deep technical expertise.

My commitment to this goal is reflected in developing platforms that allow businesses to deploy, tune, and monitor AI models with minimal technical knowledge, making AI-driven insights and automation accessible to companies of all sizes.

Conclusion

Efficient, cost-effective AI inference is a game-changer for modern businesses. It's no longer just an add-on; it's a strategic necessity for staying competitive in today's digital landscape. By embracing edge computing, optimising infrastructure, ensuring data security, creating strategic partnerships, and simplifying AI deployment, businesses can unlock the full potential of AI applications in real time.

Simply put, the future of AI is happening now, and inference is at the heart of it. ■



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

STAY CONNECTED

Improve Your Network Connectivity!

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

Mobile Mark (Europe) Ltd

Tel: +44 1543 459555

www.mobilemark.com

Email: enquiries@mobilemarkeurope.com

Satellite internet enhances ferry journeys in Orkney

In a pioneering initiative, Scottish ferry passengers in Orkney can now enjoy complimentary ultra-fast internet access, thanks to an innovative satellite-based connectivity pilot.

This marks the UK's first deployment of satellite internet on ferries, supported by the Scottish Government and managed by the Scottish Futures Trust, in partnership with Orkney-based CloudNet IT Solutions, Orkney Islands Council, Orkney Ferries, and Highlands & Islands Enterprise. The nine-month pilot focuses on the Outer North Isles ferry routes operated by Orkney Ferries, aligning with the Scottish Government's strategy to bolster community resilience, encourage population retention, and foster regional growth in remote areas. The initiative aims to demonstrate the tangible benefits of high-speed connectivity for maritime public transport, with the potential to expand across other Scottish routes.

"This innovative technology has enormous potential to improve travel for island communities and visitors alike. By trailing advanced connectivity on public transport, we are making journeys more productive and enjoyable while addressing the digital divide in rural areas," says Business Minister Richard Lochhead.

Mobile network limitations

Historically, the vessels relied on mobile network services for internet access. While functional, these systems faced limitations in terms of speed and coverage, particularly in remote areas where the proximity to cellular towers significantly impacted connectivity. Notably, some of the vessels serve two remote islands — North Ronaldsay and Papa Westray — twice a week, providing essential lift-on/lift-off services for supplies and support, and due to their geographic

locations, mobile connectivity becomes limited for all.

Operating on three ferries in northern Scotland, this public sector-funded pilot project enables travellers to work remotely, stream entertainment, shop online, and browse seamlessly. The service not only enriches passenger experience but also empowers ferry staff with improved operational tools, including streamlined back-office functions, maintenance management, and electronic transactions. Moreover, during adverse weather conditions, the onboard internet becomes a critical tool, providing captains with real-time weather and sea condition updates to ensure safety and efficiency.

Harnessing LEO for superior connectivity

The project leverages low Earth orbit (LEO) satellites, delivering speeds exceeding 200Mbps. The satellite constellation comprises over 7,000 satellites orbiting approximately 800 miles above Earth, each passing overhead every 10-15 minutes. Ferries' onboard terminals automatically establish connections with the nearest satellite. Wi-Fi technology then distributes the high-speed internet throughout the vessels, providing consistent, reliable service regardless of weather conditions or remote location.

During the pilot, it became apparent that these systems, due to the nature of their connections and their use of bulky USB-C type connectors, do not lend themselves to comfortably routing cables through marine vessels. Additionally, given the age of the fleet, these vessels were not equipped for cable dressing like the newer vessels, where Roxtec water seals are more suitable for weatherproofing the vessels. Due to the connectors not fitting through the ingress



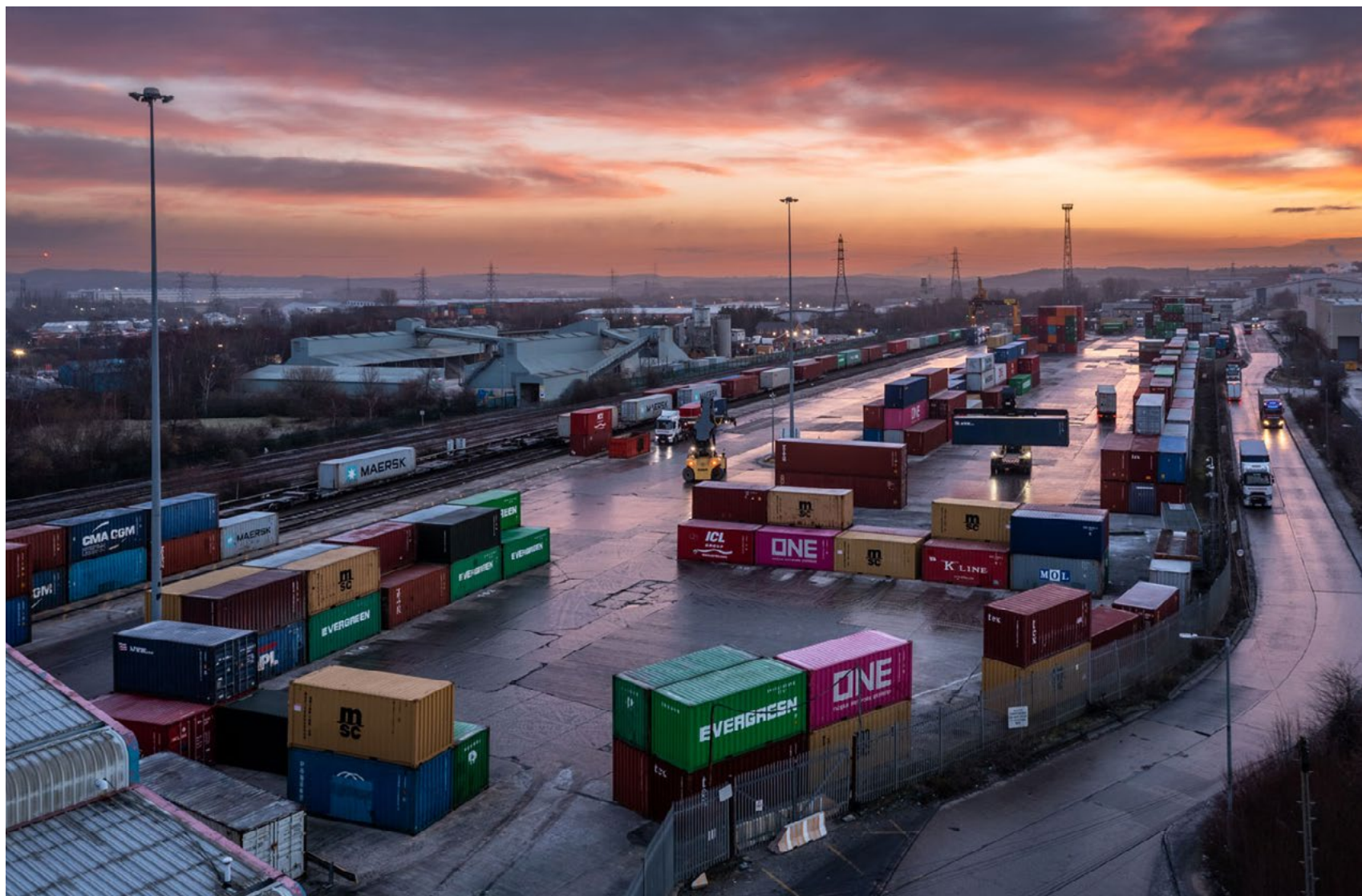
points because of the size of the ingress and the bulky connectors, CloudNet had to employ a novel approach: splitting the

cables, routing them into the ships, and re-terminating the cables using high-grade Cat7 connectors and IP68 waterproof glands. This approach made it easier to install the comms cables. It was tested and certified to meet Cat7 standards.

The successful integration directly into the bridge of each vessel allowed for seamless Wi-Fi distribution throughout key areas, including the bridge, staff quarters, passenger lounges, the crew deck, and the engine rooms. The Wi-Fi connectivity plays a critical role in enhancing operational efficiency, enabling online access to marine navigation systems, real-time weather updates, and the management of passenger manifests. The crew can also utilise the system for essential business communications, and, during their off-duty hours, for connecting with friends and family.

Currently, there are no restrictions on the bandwidth for the ship's business operations, public Wi-Fi remains a shared and freely accessible solution for passengers.

"Our goal is to elevate the digital experience on Orkney ferries, ensuring passengers can access essential online services. This initiative not only benefits travellers but also enhances operational efficiency and supports Scotland's broader digital strategy," says CloudNet IT Solutions' Director, Greg Whitton. ■



Empowering freight logistics

Freightlink, a premier freight ferry and tunnel ticketing agency, serves over 1,000 routes across more than 50 countries, supporting couriers, hauliers, manufacturers, and various other enterprises of diverse sizes.

With a partnership spanning over a decade, Evolve has been a trusted technology provider for Freightlink, offering ongoing support and solutions.

“Evolve determined that adopting a cloudbased infrastructure would best serve Freightlink’s future. The implementation involved deploying a Microsoft Azure server environment complemented by an M365 Intune setup.”

Recently, Evolve undertook a comprehensive review of Freightlink’s existing IT infrastructure to address rapid business growth and evolving operational demands, particularly emphasizing scalability and remote work capabilities. Recognizing the importance of an adaptable IT environment, both companies collaborated closely to identify the most effective future-proof solution.

On-premises upgrade or cloud migration?

Leveraging their deep understanding of Freightlink’s operations, Evolve’s IT team proposed two primary options after detailed analysis. The first involved

upgrading their existing on-site physical server infrastructure, aiming to improve capacity and performance. The second, more strategic choice, was to migrate to a cloud-based setup, offering enhanced flexibility and scalability.

Evolve’s goal was to recommend a solution aligned with Freightlink’s growth ambitions and operational needs.

After thorough consultation, Evolve

determined that adopting a cloud-based infrastructure would best serve Freightlink’s future. The implementation involved deploying a Microsoft Azure server environment complemented by an M365 Intune setup. This transition delivered multiple advantages. Microsoft Azure provides advanced security features that safeguard Freightlink’s data and applications from potential threats, ensuring the integrity and confidentiality of critical information. The cloud environment also allows for seamless scalability, enabling the company to quickly adjust resources in response to changing business demands without the need for extensive infrastructure modifications. Additionally, with Azure and M365 Intune, employees can securely

access systems from various locations, supporting flexible working arrangements and improving overall productivity. Furthermore, migrating to the cloud reduces the need for on-site server maintenance, which decreases downtime and operational overhead, leading to more efficient and reliable IT operations.

Securing the future

Security remained at the core of Evolve’s approach, ensuring that Freightlink’s

entire IT ecosystem was resilient and protected. Since completing the migration, the benefits have been tangible: a 33% reduction in monthly support tickets indicates improved system stability and user satisfaction.

This strategic move to a cloud-based infrastructure not only enhances Freightlink’s operational efficiency but also positions the company for scalable growth and remote working agility, essential for staying competitive in a dynamic logistics landscape. ■





Enterprise networks need bulletproof backup strategies to succeed

Iwona Zalewska, Regional Director for UK & Ireland, DRAM Business Manager, EMEA Region, Kingston Technology Europe

In today's digital-first enterprise environment, organisations operate across multiple locations, platforms, and networks. With employees connecting remotely, collaborating from branch offices, or accessing systems via mobile endpoints, enterprise networks have become both expansive and vulnerable. Which is why, with cyber threats escalating, backup strategies are no longer optional - they are fundamental to continuity.

Enterprise data loss: a business-level threat

Corporate networks have enormous volumes of often sensitive and mission-critical information. Yet, data loss can still result from something as mundane as human error, as menacing as a ransomware attack, or as unpredictable as a power surge or flood. Despite this mounting risk, backup negligence and secure data storage remains a blind spot for many enterprises, with the cost of data breaches spanning operational downtime, reputational damage, regulatory fines, and in worst-case scenarios, permanent business closure. A study by Censuswide for Beaming, found that up to a quarter of businesses do not back up their company data at all, while 12% maintain a single copy of data, stored either on individual computers, or on a single server. In this context, a robust, strategic backup approach using storage technology that is fit-for-purpose isn't just IT hygiene — it's a core part of enterprise risk management.

Why backup strategies fail in enterprise networks

Enterprises often underestimate or under-resource their backup planning for several reasons:

- **Complexity of infrastructure:** As companies expand, they accumulate multiple systems, data centres, and cloud environments. Without centralised visibility, ensuring consistent backup across all endpoints and networks becomes a logistical headache.
 - **Budget misalignment:** Data protection budgets are often seen as cost centres, not as investments. Some IT departments are left to 'make do,' leading to patchwork solutions and underfunded data storage.
 - **Overconfidence in redundancy:** Many firms believe that high availability systems and RAID arrays offer sufficient protection. While redundancy limits system downtime, it doesn't protect against threats like ransomware or insider sabotage that can encrypt or destroy all connected systems simultaneously.
 - **Outdated technology:** Legacy backup hardware or outdated software may not integrate well with cloud-native platforms or newer business applications, leaving entire datasets exposed.
 - **Lack of defined ownership:** In some networks, no one department takes full accountability for backup strategy, leading to inconsistencies, missed schedules, and insufficient coverage.
- **3 copies of data:** Maintain three separate copies — your primary data and two backups. This redundancy ensures that if one copy is lost or corrupted, you still have two fallback options.

Files necessary for day-to-day business continuity.

- **Regulated or legal records:** Data subject to GDPR, HIPAA, or other compliance mandates.

“Enterprises should deploy automated backup software configured to specific operational schedules and compliance requirements. Additionally, regular testing of backups — both file integrity and restore speed — is critical.”

- **2 different storage media:** Store backups on two different types of media (e.g., a local server and an external encrypted SSD). This prevents a single type of hardware failure or malware strain from compromising all data copies.
- **1 off-site copy:** Keep at least one backup copy off-site, ideally air-gapped from your network. This is crucial for recovery after physical disasters or ransomware attacks that target network-connected devices.

This model is straightforward to implement but extremely powerful in safeguarding enterprise operations.

Segmenting backups by sensitivity and importance enables targeted protection and more efficient recovery.

Automation and testing

Automation is key in large-scale environments. Manual backups are more likely to be affected by human error and inconsistency. Enterprises should deploy automated backup software configured to specific operational schedules and compliance requirements. Additionally, regular testing of backups — both file integrity and restore speed — is critical. A backup that can't be restored is as bad as no backup at all.

More than a technical afterthought

For enterprises managing hybrid cloud environments, international offices, and distributed teams, a resilient backup strategy is not a technical detail — it's a way of mitigating risk. The ROI is undeniable: avoiding downtime, slashing ransomware fallout, and maintaining compliance all deliver tangible cost savings.

Backup should be a daily discipline for every enterprise, but it starts with investing in the right storage medium to keep data secure. Research the benefits of external encrypted SSDs to determine the model best suited to the company and implement the 3-2-1 back up method as an operational imperative. The question is no longer whether your enterprise can afford to back up its data. It's whether you can afford not to. ■

A simple, powerful strategy - the 3-2-1 backup rule

The 3-2-1 approach is simple and reliable. It's a scalable, adaptable framework that ensures enterprises can withstand failures, disasters, and attacks across large, networked environments. Here's how it works:

Taking the next steps

Enterprise ransomware incidents are particularly devastating because attackers often target not only operational data but also connected backups. Without an off-site, offline copy, companies may be forced to pay ransoms or risk losing sensitive information permanently. By air-gapping one backup copy — typically stored on an external encrypted SSD — organisations create a safety net that is out of reach of attackers. Should a ransomware event occur, IT teams can isolate and restore clean data from the drive, resuming operations with minimal disruption. Businesses should also conduct a thorough inventory of their data assets and prioritise backups for:

- **Sensitive or proprietary data:** Intellectual property, customer records, and strategic plans.
- **Essential operational data:**





NEVER PAY FOR JUST SD-WAN AGAIN

Hyper-fast up to 1Gbps SD-WAN comes as standard with every OMNIA connection & protection solution

www.sdwan-solutions.global



Mastering SD-WAN deployment

Anthony Senter, CEO, & Toby Sturridge, CTO, SDWAN & SASE Solutions

Deploying SD-WAN can transform business connectivity, improve application performance and reduce costs - but success depends on careful planning and execution - and most importantly the expertise and experience of the provider.

Define clear business objectives: Start by identifying your primary goals: improved performance, cost reduction, enhanced security and better remote connectivity. Tailoring your SD-WAN deployment to these objectives ensures the solution delivers the intended value. If you're looking for digital transformation, you need essential underpinning technologies like SD-WAN and all connected businesses need robust cybersecurity and data assurance.

Prioritise security from the outset: Ensure your SD-WAN solution includes robust security features such as end-to-end encryption, firewalls, segmentation and support for zero trust models. Consider additional security tools if built-in features are insufficient for your risk profile.

Assess your existing network infrastructure: Conduct a thorough audit of your current WAN setup, including bandwidth usage, application types, performance bottlenecks and security protocols. This helps identify where SD-

WAN can address specific challenges and guides configuration decisions.

Select a proven expert SD-WAN solution and provider: Evaluate solutions based on scalability, built-in security, cloud integration and support services. Not all SD-WAN vendors offer the same features or support, so choose one that aligns with your business needs and your future plans.

Look for innovative solutions: Look closely at innovative solutions. The usual Big Tech providers often do not score highly on individual design, customer service and support (both pre and post sales). Some globally recognised names have consistently scored poorly on security, while others have 5-minute failover times - if an SD-WAN solution doesn't have sub-second failover your business is likely to experience costly downtime.

Seek flexible payment and contact terms: Monthly payment terms (PAYG) are becoming more common recently, however there are often large up-front costs and initial outlays that can make SD-WAN prohibitive for smaller businesses. If you're an SME check that you provide SD-WAN for smaller businesses, and crucially, give you and your team the support that is required for SMEs who often have smaller IT teams.

Pilot and phase your deployment: Begin

with a POC and pilot program to test SD-WAN in a controlled environment. This allows for real-world adjustments before a full rollout, minimising disruption and ensuring the chosen solution meets your needs.

Plan for redundancy and reliability: Leverage SD-WAN's ability to use multiple connections (broadband, MPLS, LTE) and configure automatic failover. This ensures high availability and minimizes downtime in case of network failures. Use intelligent path selection and application-aware routing to ensure that business-critical applications (like VoIP, video conferencing and SaaS) always have the necessary bandwidth and lowest latency.

Ensure seamless integration with existing infrastructure: SD-WAN should integrate seamlessly with your current network and cloud services. Consider compatibility with legacy systems and ensure the solution can support your cloud and SaaS connectivity strategies.

Seek references from potential providers' customers: Check your provider's integration experience and ask to speak to current customers about integration and support. Seamless integration is easier said than done - several well-known tech providers are revising their SD-WAN offers, due

to the intricacies of integration. This is where real experts with experience stand out from the crowd.

Continuous monitoring and optimisation: After deployment, continuously monitor network performance and application experience using analytics tools. Ongoing optimisation ensures the network adapts to changing business needs and maintains high service levels.

Invest in training and support: A truly collaborative and supportive SD-WAN provider should happily upskill in-house IT teams to ensure the project runs smoothly before, during and after installation.

SD-WAN bundles will reduce time, cost and complexity: Just as continual fast connectivity - like that provided by true SD-WAN - is a given need for 99.9% of businesses, so is cybersecurity, data, voice and video encryption, XDR and secure access to multi-clouds and IoT. Progressive providers are creating technology bundles with their SD-WAN offers, knowing customer concerns about integration, multiple vendors and dozens of solutions.

By following these best practices, businesses can maximise the benefits of SD-WAN, ensuring a secure, reliable and cost-effective network transformation. ■

PRODUCTS

Wavenet provides a range of options for a SD-WAN delivering optimised performance, security and efficiency of network traffic.

The solution can be fully managed by Wavenet and can be applied to numerous variants of network underlay, including ADSL, SOGEA, FTTC and others. Wavenet helps retailers, banks, hospital

networks, and many other distributed enterprises to deliver high-availability services to their end users in the middle of ever-changing requirements and increasing internal growth.

The company can help clients securely connect branch locations and synchronise security settings across thousands of sites using Wavenet's extensive engineering

network and collective wealth of experience. Wavenet is also the first partner in the UK to achieve the Cisco SSE designation and hold 4 Cisco Powered Service Designations: Secure Access Service Edge (SASE), Security Service Edge (SSE), Meraki SD-WAN and Managed Security. Additionally, it is a Fortinet MSSP Expert Partner with specialisations in SASE, SD-WAN, and

Security Operations.

As a Crown Commercial Service (CCS) supplier, Wavenet works across various frameworks, including the Network Services 3 (RM6116) framework and HSCN Access Services DPS (RM3825), ensuring full HSCN compliance.

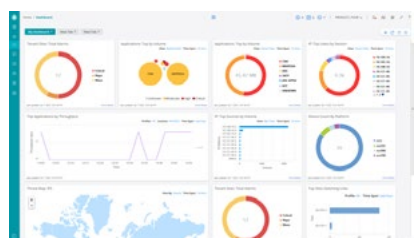
For more information, visit: Wavenet.co.uk/networking

The Stream Managed SD-WAN offers a seamless migration from traditional MPLS or IP VPNs to a modern, cloud-ready, AI-driven, application-aware network. It securely connects corporate sites, remote users, and hybrid multi-cloud environments ensuring optimal application performance and guaranteed Quality of Experience (QoE).

It features dedicated peering agreements with major UK Voice Carriers for SIP termination and direct connections to leading cloud providers like Microsoft Azure, AWS, Google Cloud, IBM, Oracle, and SAP, ensuring optimal routing for critical applications and services.

Management is streamlined through the cloud-based Contrail Service Orchestrator (CSO), which offers centralized, user-friendly control over security policies, application routing, and device management across physical and virtual appliances deployed in offices, branches, data centers, and cloud environments.

Real-time monitoring capabilities provide comprehensive insights into network traffic, devices, applications, and security events, enabling IT teams to maintain visibility and control. Zero Touch Provisioning (ZTP) automates device deployment, minimizing manual intervention and reducing deployment costs.



Backbone Connect's SD-WAN solutions provide a modern, flexible approach to wide-area network connectivity, offering secure, high-performance solutions tailored to meet your specific business needs.

Utilizing advanced technologies and integrating AI capabilities, Backbone Connect designs, deploys, and supports SD-WAN solutions aligned with the business' strategic goals. A dedicated service team maintains the network's optimal operation, allowing the client to focus on growing business.

Backbone Connect leverages industry-leading platforms such as Fortinet and

Cisco Meraki to deliver top-tier security, performance, and scalability. Whether the aim is to strengthen security, improve network performance, or enable rapid expansion, Backbone Connect offers the expertise and support necessary to achieve objectives.



Jisc's Managed SD-WAN service provides a flexible and efficient way to connect to the Janet Network, the UK's national research and education network (NREN), supporting enterprise digital transformation.

SD-WAN utilizes software to optimize WAN performance, replacing traditional hardware-based solutions. Unlike conventional networks that depend on physical routers and manual configuration, SD-WAN separates hardware from the control system, enabling centralized management that is more efficient and easier to oversee.

Through Jisc's partnership with BT and Fortinet, organizations can extend connectivity beyond the physical campus boundaries to remote and underserved areas, integrating sites across the community. Setting up an SD-WAN connection is faster than traditional networks and requires no additional

infrastructure, allowing rapid deployment to meet evolving organizational needs.

The service includes built-in security features of the Janet Network, such as foundational DDoS protection and JNRS, enhancing cybersecurity posture.

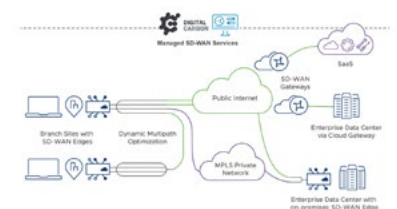
The benefits of SD-WAN are substantial. It provides quick and straightforward access to the Janet Network without the need for new infrastructure. It ensures secure and reliable connectivity through edge-based firewall management and advanced security measures, protecting against threats and enforcing security policies effectively. The scalable infrastructure supports multi-site and inter-site connectivity, allowing rapid deployment and configuration of geographically dispersed locations within a unified network architecture - delivering greater performance, flexibility, and operational efficiency.

Managed SD-WAN by Digital Carbon simplifies and reduces the risks associated with network transformation.

It provides a centralized, automated platform that securely coordinates workloads across a variety of connectivity types, offering full visibility and control. As a vendor-independent provider, Digital Carbon aggregates bandwidth from multiple transport technologies, delivering a single managed resource with enhanced centralized management. This approach enables customers to streamline operations, improve security, and increase network viability.

Managed services include proactive monitoring of both the underlying network infrastructure and the SD-WAN platform itself. Digital Carbon promptly alerts customers to any issues and escalates service problems to the appropriate vendors, ensuring swift resolution. Customers benefit from a single point of contact for all service inquiries, simplifying communication and support.

Digital Carbon's flexible managed SD-WAN solution allows businesses to choose and modify network components as their needs evolve. They provide 24/7 monitoring and management, ensuring continuous service delivery and performance.





Please meet...

Jason Legget, Public Sector and Enterprise Solutions lead at Connexin

Who was your hero when you were growing up?

As a kid, my hero was the original Inspector Gadget—part detective, part tech pioneer. Watching him tackle problems with ingenious tools was inspiring - literally a walking IoT device before the concept of IoT gained widespread popularity. I mean, who wouldn't want a gadget-laden hat that could optimise their day with a simple "Go,Go,Gadget" command?

What was your big career break?

In the early 90s, being head-hunted from Teesside University by Comcast to launch one of the UK's first Business ISPs. I was working on the project taught me the power of translating complex technical solutions for non-tech-savvy stakeholders. Selling "the art of the possible" with the internet became my superpower and lifelong skill.

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

"Don't just work hard, work smart." I've learned that true success lies in thoughtful strategy, not just relentless effort. It's about understanding the bigger picture, using resources wisely, and creating solutions that deliver impact without unnecessary friction. Funnily enough, it's the leading principle behind IoT and data-driven decisions and it's been my North Star ever since.

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

At Connexin our purpose is to create smarter, more connected solutions that improve lives, build stronger communities, and address the country's biggest challenges.

In an alternative life, I'd probably stick closely to this realm but within public services itself. Improving the way that community's function through innovation and helping every member shine. Delivering better outcomes at lower costs is a challenge that feels vital.

Innovation isn't just about technology; it's about empowering people and fostering change where it's needed most. There's nothing more rewarding than seeing the tangible impact of those efforts in the places we call home.

Where would you live if money was no object?

I live in a great place, with an amazing partner, so as long as we can travel and see the world as we get older, I'll be content. The real wealth is in the experiences we create and the security we build for those we love.

So, if money were no object I would live exactly where I do now, but I'd like to think I'd be the benevolent mastermind of opportunities, working with people, supporting my family, and helping the community thrive. Of course, I'd still indulge in globetrotting with my partner, sampling exotic cuisines, and pretending to know more about art than I do.

The Rolling Stones or the Beatles?

Choosing between the Stones and the Beatles is impossible for a non-fan like me. As a Scouser, I'd naturally lean toward the Beatles, but my heart takes me off-piste to Prince. He was everything: innovative, genre-defying, and utterly captivating. His music ignited my love for diverse genres and demonstrated the limitless power of creativity. To quote the man

himself, sometimes you just have to embrace life and "Let's Go Crazy."

What would you do with £1 million?

First, I'd make sure my kids' education and futures are secure, and my immediate family has everything they need. £1 million doesn't stretch as far as it used to, but I don't need much myself.

Beyond that, I'd invest in projects that make a real difference—helping communities innovate, tackling environmental challenges, and ensuring everyone has a

chance to shine. After all, the ultimate luxury isn't yachts or private islands, it's leaving the world a bit better than you found it (though a yacht might occasionally help with that).

What's the greatest technological advancement in your lifetime?

It's got to be the internet, without a doubt. It's the foundation of everything: from IoT to cloud computing, to answering life's most pressing questions—like whether you really need to boil potatoes before roasting them (answer: yes). Without it, where would we be?

The internet has transformed how we live in ways both brilliant and bizarre. It's given us Teams video calls that let you wear pyjama bottoms during serious meetings, online shopping that lets you impulse-buy anything from Temu at 2 a.m., and the life-saving genius of being able to diagnose a mild headache as a rare tropical disease via WebMD!

The internet isn't just a tool; it's the great equaliser, the ultimate procrastination enabler, and the reason we'll never again need to remember a friend's birthday without Facebook reminding us. ■

TCCA CRITICAL COMMUNICATIONS WORLD 2025

17-19 JUNE 2025
BRUSSELS EXPO, BRUSSELS, BELGIUM

WWW.CRITICAL-COMMUNICATIONS-WORLD.COM

TCCA CRITICAL COMMUNICATIONS WORLD

REGISTER NOW

PLATINUM SPONSOR: **MOTOROLA SOLUTIONS**

GOLD SPONSOR: **ERICSSON**

ORGANISED BY: **MA Exhibitions**

PRESENTED BY: **TCCA 30**

HOST OPERATOR: **astrid**