MAY 2023
networkingplus.co.uk

NETWORKING+

Web scraping
Revolutionising data use
Aleksandras Šulženko, Oxylabs, p5

Securing remote devices
Taking a zero trust approach
Dave Waterson, SentryBay, p6

Questions and answers
Be open to continue to learn and develop
Jonathon Sharp, Britannic, p16

Taking stock of 5 years of GDPR

Moving on from an era of almost cavalier disregard for data protection and privacy, the General Data Protection Regulation (GDPR) – which has ushered in stringent security requirements for all data – is celebrating its five-year anniversary this May.

However, despite threats of fines, compliance has not been straight forward for all enterprises.

"Learnings from the COVID-19 pandemic have raised concerns about new public health and data considerations that should be factored into future legislation," says Michael Covington, VP of strategy at Jamf. "Additionally, the post-Brexit version of GDPR for the UK is still a work in progress, as is a firm stance on how data can be shared between EU member states and 'partner' countries."

What GDPR means for enterprises continues to evolve with the expanding use of AI/ML and biometrics. Earlier in May it was revealed that Mobile World Congress (MWG) organiser GSMA fell foul of GDPR rules around biometric data, resulting in a €200,000 penalty. To register for the 2021 event, attendees were required to upload their passport data, leading to complaints. The organisation was determined to have failed to demonstrate due diligence before collecting biometric data from show attendees, infringing Article 35 of GDPR.

"As defined by Article 4 of GDPR, biometric data is a form of personal data – therefore, businesses must carefully and securely manage it," says Eduardo Azanza, CEO at Veridas. "With the rise of biometrics and AI, the focus on data protection and privacy has never been more important. Trust in biometric solutions must be based on transparency and compliance with legal, technical, and ethical standards. Only by doing this, can we successfully transition to a world of biometrics that protects our fundamental right to data privacy."

Compliance with GDPR regulations is also still raising new challenges around transatlantic data transfers. Just a few days ago, Ireland's Data Protection Commission (DPC) fined Facebook parent Meta a whopping £1 billion, the largest ever fine handed out for breaching GDPR. The kerfuffle related to a legal challenge over concerns that European users' data is not sufficiently protected from US intelligence agencies when transferred overseas.

The DPC ruled that Meta had infringed GDPR by continuing to transfer EU user data to the US without proper safeguards in place. The CJEU ruled that data leaving the EU must have the same level of protection as it would have under GDPR when it reaches its destination outside the EU.

"We are … disappointed to have been singled out when using the same legal mechanism as thousands of other companies looking to provide services in Europe," wrote Nick Clegg, Meta president of global affairs, and Jennifer Newstead, Meta chief legal officer, in a blog post.

A spokesperson for the European Commission said that it hoped a new framework for transatlantic data transfers would be "fully functional by the summer" which would provide the "stability and legal certainty" sought by US tech companies.

"This fine concerns some of the most legally complex issues that data privacy practitioners have ever had to tackle," shares Janine Regan, legal director for data protection at law firm Charles Russell Speechlys. "The level of the fine is staggering particularly because it's not an issue that any one company can resolve on its own and given that there is political agreement on both sides of the Atlantic to solve the issue."

Half a decade after its implementation, it's clear that there's still work to be done to iron out GDPR compliance challenges for enterprises. ■

Largest temporary private 5G SA network deployed for Coronation

5G technology tested in Loch Lomond at the Scotland 5G Centre testbed was deployed with BBC R&D to support the live broadcasting of His Majesty King Charles III's Coronation.

The University of Strathclyde software-defined radio (StrathSDR) team and Neutral Wireless deployed the largest temporary private 5G standalone network of its type at the King's Coronation. This network was used by 20 leading broadcasters, including BBC, CBS, Sky and CNN. The company set up eight 5G cells along The Mall, providing reliable and uncontested coverage from Buckingham Palace to Admiralty Arch. This network delivered 1Gbps of wireless connectivity, carrying high definition (HD) video from wireless cameras to production facilities around the world.

"The Scottish Government's investment via our Scotland 5G Centre has made it possible for the Neutral Wireless team to break a new world record by broadcasting such an historic occasion to millions of people around the world over a 5G network," said Scottish Government innovation minister Richard Lochhead. "This outstanding achievement demonstrates once again how 5G technology can help transform Scotland's economy by driving innovation and enhancing our global competitiveness."

To provide wireless HD cameras for live events, broadcasters may use point-to-point radio connections or use the public mobile networks with purpose-built multi-connection cellular bonding solutions. However, point-to-point links can be expensive, and using the public mobile networks can be challenging at large events, where large crowds can cause congestion and put a strain on network resources.

In addition, professional high-definition video requires high-capacity networks with a high upload speed, whereas public networks are designed with a focus on serving data downloads to thousands of connected devices. The high quality private 5G network solved these issues, allowing camera operators to get close to the action and engage with the public without being inhibited by wires, whilst still streaming high-definition live footage. The network was also used to provide connectivity for live BBC radio contributions.

"The Coronation filming shows the enormous scope of 5G technology, being trusted to facilitate the worldwide broadcast of a historical moment," said Ian Sharp, head of business development at the Scotland 5G Centre. "While all eyes were on London, behind the scenes, Scottish innovation and testing in the S5GC rural testbed at Loch Lomond helped the broadcast of this important day to go smoothly. This achievement showcases the transformative potential of 5G, as well as the need for testbed facilities and innovation hubs to support industry with real world applications." ■

NetApp provides data pipeline boost for Aston Martin Aramco Cognizant Formula One Team

As the Formula 1 contest heats up, Aston Martin Aramco Cognizant Formula One Team has partnered with NetApp to optimise the AMF1 Team's application performance and cost – on and off the track.

Enabling a fast, efficient data pipeline, alongside a simplified and unified management plane, NetApp's technology is supporting the AMF1 Team to spot opportunities for driving improvement in real-time.

The aim of the NetApp transformation partnership project with the AMF1 Team was simple: to make their cars go faster. The project focussed initially on infrastructure and the building out of the data fabric, now the team are using data insights to focus on that all-important title.

NetApp has worked with AMF1 Team to implement FlexPod as a trackside converged infrastructure platform, which replaces multiple singular points of failure, improves availability and performance, while also removing legacy systems.

This in turn reduces weight and, therefore, has a positive impact on reducing the carbon footprint.

FlexPod has produced results in five key areas:

Performance: FlexPod has allowed AMF1 Team's performance software group to tap in to compute power and storage to develop a Kubernetes cluster at track to allow the team to analyse data at a faster rate with no bottlenecks.

Reliability: By having a high-performing FlexPod solution with two redundant converged infrastructure platforms, AMF1 Team can run all the systems but can load balance across both FlexPods for increased performance.

Resiliency at a host level is achieved with three hosts on each FlexPod, redundant network switches and full N+1 resiliency on cables both across one FlexPod and then between racks and FlexPod.

Continuous improvement: The IT team must constantly push to enable the whole team and the car to have better agility, greater speed, and improved reliability. With the speed that telemetry data is being sent from trackside to factory being reduced from 20 minutes to less than 10 minutes, engineers at the AMF1 Team factory can analyse the data at speed and adjust if needed.

This is being achieved using NetApp SnapMirror technology which is transferring the data back to the factory to Mission Control at a significantly improved rate.

Security: Protection is a core principle to safeguard the most valuable asset within the team; their data. It is important to make this process easier and more informative.

AMF1 Team uses Cloud Secure, a feature of NetApp Cloud Insights which provides a simple turnkey solution to enhance their ability to detect ransomware and provide user data access auditing. It analyses data access patterns to identify risks from ransomware attacks. Moreover, NetApp Cloud Secure also reports access activity from insiders, outsiders, ransomware attacks, and rogue users. Advanced reporting and auditing make it easy to identify violators and possible threats, emabling action to be taken quickly.

Speed towards sustainability: Formula 1 set out its sustainability plan to have a net-zero carbon footprint by 2030. For the AMF1 Team, as a key player in this industry, the introduction of FlexPod is contributing to the team's sustainability efforts in multiple ways.

In the AMF1 Team's new Silverstone smart factory, NetApp Cloud Insights technology helps consolidate the company's older, less efficient systems and provides essential temperature and power monitoring, enabling AMF1 Team to monitor and minimise power consumption.

"NetApp high performance FlexPod are fundamental to our operation at the track," said Clare Lansley, chief information officer, Aston Martin F1 Team. "

"They are therefore given kid-glove treatment and high protection as we fly them to races around the world. As we use data to improve our performance and go faster, NetApp's work with the AMF1 team is vital to this success," added Lansley. ■

Euronics to gain IoT cloud platform for automation at more than 50 shops

SES-imagotag has been selected to roll-out the VUSION IoT Cloud platform in more than 50 Euronics shops across the UK, within their Combined Independents (Holdings) Ltd (CIH) chain.

After a successful pilot phase in 20 stores, Euronics, which accounts for the largest consumer electronics store footprint in the UK, will consider expanding the use of the VUSION solutions to their 600+ locations throughout the country in the medium term.

The implementation of SES-imagotag's VUSION IoT Cloud platform will enable Euronics United Kingdom stores to better manage their prices and promotions, while ensuring greater responsiveness and accuracy in aisles. With VUSION, Euronics will be able to leverage digital tags to automate low-value-added tasks in-store and focus associates on customer service as well as product availability.

By adopting SES-imagotag's solutions, Euronics will be able to reduce paper consumption and deploy in-store IoT at minimal cost, with a reduced carbon footprint. VUSION's native integration with existing Cisco-Meraki infrastructure enables an optimised and hardware-efficient operating framework.

"At Euronics, our goal is to provide our customers with excellent service while offering the right price at the right time," said Steve Scogings, chairman at CIH. "To achieve that, we are committed to investing in our stores and leveraging the best technology has to offer today. With SES-imagotag, we are able to do so while being mindful of our impact on the environment, whilst maximising our impact on local communities."

"We are very proud that Euronics has selected us once again for their digitalisation journey, further strengthening our leading position in the consumer electronics vertical. To be able to help a retail chain such as Euronics in their digitalisation is a great satisfaction for us, as we commit more than ever to enable a sustainable transformation of physical commerce," said Sébastien Fourcy, SEVP EMEA at SES-imagotag. ■

EDITORIAL:

Editor: Amy Saunders
amys@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Aleksandras Šulženko, Adrian Moir, Dave Waterson, David Watkins, Dennis Mattoon, Jonathon Sharp, Ross Slogrove

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

ISSN: 2052–7373

Daisy delivers SD-WAN and cloud UC for A.S. Watson

Daisy Corporate Services has announced a multi-year managed services contract with A.S. Watson Group, the world's largest international health and beauty retailer. A.S. Watson's brands in the UK include Superdrug, Savers, and The Perfume Shop.

Daisy will provide SD-WAN, cloud unified communications, and fibre connectivity to more than 1,500 stores in the UK.

To support its digital transformation and cloud-first strategy, A.S. Watson sought to future proof it's in-store connectivity to enhance the employee and customer experience. Daisy will deliver connectivity-as-a-service via a Meraki SD-WAN solution, which will provide greater insight into network performance, support the transition to cloud-based services, and increase overall network resiliency.

In addition to upgrading A.S. Watson's underlying connectivity to SoGEA broadband and FTTP, Daisy is partnering with Cisco Meraki to expand A.S. Watson's existing Meraki WiFi network.

"We needed a flexible, agile, and secure networking solution to support our ongoing digital transformation strategy. Having a modern network will increase bandwidth at all our locations and enable us to better support new store initiatives in the future. Daisy is a proactive partner that shares our ESG values and we are fully confident they will meet our connectivity needs now and in the future," said Andrew Cobb, group IT director, A.S. Watson UK. "As more customers see the benefits of shopping both online and offline in our stores, it's really important for customers to be able to connect their devices in our shops. Customer WiFi will help with conversion and enable people to use our app or website in our stores."

"For high street retailers, fast and secure connectivity is a key piece of the digital transformation jigsaw," said Chris London, head of sales specialists at Daisy. "With our deep understanding of the retail sector, we understand the unique technology challenges and opportunities these businesses face. We are delighted to be extending our partnership with A.S. Watson to deliver innovative networking solutions that drive growth and success for its UK brands." ■

Connectivity: 79% agree rural areas are being left behind

Cradlepoint has published the findings from its State of Connectivity in Europe report in cooperation with Censuswide.

According to the report, European businesses could be missing out on billions of pounds as 74% experienced at least two hours of downtime every week. With Statista stating that an hour of downtime for a global business can cost £290,000, this constitutes a huge cost to European economies. On top of this, connectivity problems have resulted in greater operating costs for 47% of businesses, and 33% report losing potential business because of connectivity issues.

In the UK, the survey found that poor connectivity hinders progress in rural areas in rural communities, greatly affecting local businesses and economies. In fact, 84% agree poor connectivity in rural areas means they would set up a new business in a city. Further to this, 79% agree rural areas are being left behind in medical innovation due to poor connectivity, and 73% agree the NHS digital transformation strategy is being held back due to poor connectivity in hospitals.

In light of this, the UK government has recently released its roadmap for wireless infrastructure, which announced investing £40 million to drive the take up of innovative 5G-enabled services for business and the public sector.

"It is reassuring that the UK government has finally released their strategy for improving wireless infrastructure nationwide. Providing clarity and, crucially, funding for 5G and 4G planning is always a welcomed step. However, the proof will be in the execution, and these guidelines must be followed up with strong action to ensure the goals are met," said James Bristow, SVP EMEA at Cradlepoint. "While this plan is a step in the right direction, the deadline of 2030 is still several years away, and the objectives leave lots of room for improvement. For example, only getting 5G to populated areas means rural areas will continue to be left behind, often the places that need the most attention. Meaning existing digital and productivity gaps will persist in the future as well. If the government is truly determined to establish the UK as a leading nation in the world of wireless infrastructure and unlock the benefits this can bring to businesses, much more support is needed." ■

Costa Coffee selects GEP for digital transformation

Costa Coffee has selected GEP SOFTWARE, a procurement and supply chain platform, after a competitive selection process.

Costa Coffee is present in 45 countries with more than 2,800 coffee shops in the UK and Ireland. As part of its digital transformation, Costa Coffee has selected GEP SOFTWARE to transform and automate its source-to-contract procurement process for all indirect spend, encompassing sourcing, contract, and supplier risk management.

"We selected GEP because of its proven procurement software and expertise to help us continue to grow and deliver new value to our customers and shareholders," said Xavier Martinez, chief supply chain officer at Costa Coffee.

GEP SOFTWARE encompasses GEP SMART procurement software and GEP NEXXE, a next-generation cloud-native supply chain unified platform. It enables clients to drive optimum efficiency, agility, visibility, and actionable intelligence into all procurement, purchasing and supply chain functions while eliminating burdensome infrastructure and support costs to achieve maximum ROI. ■

50% of organisations were spear-phishing victims in 2022 - criminals continue to utilise targeted email attacks

Barracuda Networks Inc. has published its 2023 spear-phishing trends report, which presents propriety spear-phishing data and analysis, drawing on a data set that comprises 50 billion emails across 3.5 million mailboxes, including nearly 30 million spear-phishing emails.

Overall, the research shows that cybercriminals continue to barrage organisations with targeted email attacks, and many companies are struggling to keep up. While spear-phishing attacks are low-volume, they are widespread and highly successful compared to other types of email attacks.

50% of organisations analysed were victims of spear phishing in 2022, and a typical organisation received five highly personalised spear-phishing emails per day. Moreover, these attacks are highly successful - spear-phishing attacks make up only 0.1% of all e-mail-based attacks, but they are responsible for 66% of all breaches.

55% of respondents that experienced a spear-phishing attack reported machines infected with malware or viruses; 49% reported having sensitive data stolen; 48% reported having stolen login credentials; and 39% reported direct monetary loss. On average, organisations take nearly 100 hours to identify, respond to, and remediate a post-deliver email threat.

Users at companies with more than a 50% remote workforce report higher levels of suspicious emails — 12 per day on average, compared to 9 per day for those with less than a 50% remote workforce. Companies with more than a 50% remote workforce also reported that it takes longer to both detect and respond to email security incidents.

"Even though spear phishing is low volume, with its targeted and social engineering tactics, the technique leads to a disproportionate number of successful breaches, and the impact of just one successful attack can be devastating," said Fleming Shi, CTO, Barracuda. "To help stay ahead of these highly effective attacks, businesses must invest in account takeover protection solutions with artificial intelligence capabilities. Such tools will have far greater efficacy than rule-based detection mechanisms. Improved efficacy in detection will help stop spear-phishing with reduced response needed during an attack." ■

Home Office launches tender for ESN project

The UK Home Office has launched a tender worth up to £895 million for a user services supplier for its issue-riddled Emergency Services Network (ESN), a project which has been plagued with years of delays and escalating costs.

In a tender notice issued in May, the Home Office said that it was aiming to establish a contract for a 'user services' supplier to work in conjunction with other partners, including the mobile supplier which is currently EE.

The successful bidder will be involved in programme and project delivery, system integration, delivery of network and IT infrastructure, including a dedicated dual 4G/5G standalone mobile core network, and specifications and certification services for third-party devices and systems connected to the ESN.

Prospective bidders must submit their tenders by 19 June and the initial term of the contract lasts until the end of 2031, with the possibility of two 12-month extensions. ■

Birmingham eyes digital twins

Birmingham City Council is planning to use a digital twin in its ambitious programme to achieve net zero carbon emissions for the entire city in the near future.

The project will gather real time data from sensors on features such as energy output, pollution and traffic congestion. This data will feed into a virtual model to run simulations, study performance issues, and generate possible improvements in how the council runs it services in its efforts to achieve net zero.

"This is a great way of helping us tackle the big challenges facing the city, seeing what works and where the problems are using real time data. That way we can invest intelligently, making sure we can be even more confident of results that will help our residents," said Cllr Jayne Francis, Birmingham's cabinet member for digital, culture, heritage, and tourism. "There will be some really pioneering work happening in east Birmingham, tied to our inclusive growth programme, unlocking opportunities for local tech and social enterprises, which traditionally attract people from more disadvantaged communities." ■

London police gain body-worn cameras to maximise productivity

The City of London Police will roll out Motorola Solutions' VB400 body-worn cameras to its entire police force.

The new VB400 body-worn cameras will integrate seamlessly with the police force's existing ecosystem of technologies to maximise end-to-end safety, security, and productivity. Collaboration with the Pronto mobile digital policing platform will align video footage with other incident report information and connectivity with a wide range of sensors will automate recording when critical events occur, such as an officer pressing the emergency button on their MXP600 TETRA portable radio. ■

Word on the web...

Three smart cost-cutting techniques for data storage

Adrian Moir, senior product management consultant & technology strategist, Quest Software

To read this and other opinions from industry luminaries, visit www.networkingplus.co.uk

Nine projects that prove web scraping is revolutionising data use

Aleksandras Šulženko, product owner, Oxylabs

Web scraping is revolutionizing data applications. Advanced collection practices allow higher levels of data extraction at faster rates, enabling new opportunities in healthcare, finance, ecology, politics, and economics.

New data sources are continuously being created as people increasingly conduct business, personal, and professional transactions online. As these sources expand, researchers are finding new opportunities to develop their research and obtain new insights. Researchers are improving their findings, deriving increasingly accurate conclusions, and producing better solutions to problems affecting people, businesses, and governments.

How researchers obtain high-quality data

Legacy data sources include journals, purchased data sets, and information collected manually from the internet. Besides being resource-intensive, these methods typically require hours of manual entry into spreadsheets that are tedious, time-consuming, and prone to error.

Today's research landscape is vastly superior. Researchers now access a trove of online data covering nearly every subject. Examples include financial websites with historical stock information, public databases with clinical drug trials, and online marketplaces.

Modern data gathering methods enable researchers to extract information at scale and automatically update their databases. Imagine an online resource with thousands of stocks, including historical pricing information, current news, and trading volumes - web scraping makes it possible to make thousands of data requests from that website per second and deliver the information in a spreadsheet format that analysts can easily read.

How web scraping works

Web scraping requires the creation of scripts written in a programming language to crawl websites and extract data. Alternatively, smaller or personal data extraction projects can be executed using browser extensions that parse website HTML and export the information in a spreadsheet format.

Another alternative is a web scraping API that can be easily customized. Researchers opting for this solution can quickly extract information at scale and avoid many common process challenges, allowing them to focus on obtaining insights.

Nine research projects enhanced by web scraping

Web scraping enables new research into economics, healthcare, ecology, and politics by allowing researchers to gather data from emerging online resources. Without automation, some of these projects would have been impossible to complete without hundreds of hours of manual data collection, entry, and processing.

1. Opioid-related death tracking

Oxford researchers downloaded over 3,000 PDF documents to study opiod deaths in the UK. Web scraping made it possible to scale the project considerably so they could focus on other research-related tasks. "We could manually screen and save about 25 case reports every hour," reads an article in Nature describing the project. "Now, our program can save more than 1,000 cases per hour while we work on other things, a 40-fold time saving."

Automating data collection also opened up collaboration. By publishing the database and frequently re-running the program, researchers enriched the project by sharing findings with the academic community.

2. Tracking clinical trials

The Oxford researchers studying opioid deaths in the previous example also used web scraping to gather information from clinical-trial registries to further develop their published data set tracking primary-case prescribing in England.

3. GDP nowcasting

Government entities typically announce gross domestic product (GDP) on a quarterly basis. Web scraping enables researchers to make GDP predictions more frequently.

GDP is calculated by adding consumption, investment, government, and net exports. Most of these components are higher-frequency metrics that can be scraped from online sources, allowing for the creation of models that predict GDP ahead of official announcements.

Reserve banks throughout the world currently leverage this method, including the USA, European Union, South Africa, China, Brazil and Japan.

4. COVID-19 tracking

The Bank of Japan (BOJ) actively uses alternative data - information outside 'official' government and corporate reports - to evaluate key economic sectors and develop policy. Recent applications include the collection of mobility data during COVID-19 that revealed pedestrian traffic, financial transactions, and airport visits.

5. Price inflation

Researchers from Poland gathered food and non-alcoholic beverage prices from major online retailers and created a framework to estimate inflation rates in the near term (also called a 'nowcast'). They demonstrated that accounting for online food prices in a simple, recursively optimized model effectively predicts inflation and even outperforms traditional approaches.

6. Unemployment insurance claims

Unemployment reached all-time highs during COVID-19, highlighting the need to predict jobless rates to estimate unemployment claims. Researchers in a recent paper explored information sets and data structures from the spring of 2020 to predict job losses in the USA and how they can be used to forecast unemployment claims.

7. Ecological insights

Environmental researchers are extracting data from Google Trends, news articles, and social media to get insights into species occurrences, behaviors, traits, phenology, functional roles, and abiotic environmental features. Referred to as ;iEcology', this emerging research approach aims to quantify patterns and processes in the natural environment using digital data from public sources.

8. Political sentiment

Internet users are becoming increasingly vocal about political matters on social media networks and public forums. Political groups are leveraging this trend by scraping online sources to identify critical issues and using that data to formulate campaign content.

9. ESG data

Environment, social, and governance (ESG) investment guidelines are designed to address climate change concerns, greenhouse gas emissions, water management, and waste reduction. Investment managers and financial analysts can assess an entity's adherence to these guidelines by scraping online databases containing ESG data. ■

Securing remote devices means taking a zero trust approach from the start

Dave Waterson, CEO, SentryBay

The expected mass return to the office has not materialised, and the emphasis now is on supporting a hybrid workforce in the long term. At the same time, companies are under pressure to bring down costs as black clouds hover over the economy. It has made sense over the past year to introduce, or escalate, Bring Your Own Device (BYOD) policies that allow staff to make use of their own laptops or home PCs. While this is a proven way to lower capital expenditure, it doesn't come without risk, particularly for companies with large numbers of employees.

The challenge relates to a lack of control. Devices of any kind that interact with the corporate network regardless of whether it's in the cloud or on-premises, present network and security managers with a headache. How can they know the security status of a device, who else might use it, the applications that are being accessed on it, or where it is located? The other issue for sectors that are closely governed by regulations, is that unmanaged devices are unlikely to be compliant.

The risk environment

There is good reason to be concerned. Cyberattacks are on the increase regardless of which threat report you read. A rise of 28% in the third quarter of 2022 over the same period in 2021 was noted by one security company recently, while high profile ransomware attacks on key public entities continue to make headlines. The war in Ukraine has also generated an uptick in negative cyber activity this year, all of which adds up to multiple hazards for organisations.

Containerise applications to protect them

Implementing zero trust company-wide means elevating the security posture. All aspects of protecting data and applications need to be considered so that a BYOD policy can work seamlessly. Employees need to be confident that their privacy is protected when they are using their own devices, but the company has a duty to ensure those devices pose no risk to its systems, and to its own customers. The simple solutions of internet security and anti-virus software or even a virtual private networking (VPN) will not suffice. A stronger, layered defence needs to be put in place. This allows for an attack to be fended off, even if it successfully bypasses the first layer of protection.

Some companies will find that adopting zero trust is straightforward, others will not. Much depends on the existing infrastructure, the adherence to security rules and access, and the commitment to BYOD. The best place to start is with a solution, or even a set of solutions, that deliver a common security baseline. They must protect against kernel level keylogging and screen capture, but alongside that, wrap or containerise data and applications so they cannot be impacted by any other form of malware, irrespective of the device that is being used.

"Employees need to be confident that their privacy is protected when they are using their own devices, but the company has a duty to ensure those devices pose no risk to its systems, and to its own customers."

What should not be overestimated is the willingness of employees to engage with and download the security solution. It is impossible for a security or network manager to control every remote device in a BYOD environment, so the solution that is selected should be easy to implement, easy to use, and require little technical support.

Ideally, organisations should select solutions that confine applications. As I said previously, containerising applications and data as they flow in and out of the network means that malware does not have the opportunity to 'escape' and there's no necessity to identify it to defend against it. Connect this with anti-keylogging software and always-on screen protection and it puts companies well on the road to achieving zero trust. ■

While classified as simple malware, among the most dangerous types of cyberattacks come from keylogging and screen capture. Both attacks are a form of spyware and utilised by bad actors to steal sensitive personal and corporate data. A remote device which is not protected by anti-keylogging or anti-screen capture software is at risk of providing an attacker with log-in details to their own files, the online services they use, and to the data and applications hosted on their company's network as they access them.

Never trust, always verify

The National Cyber Security Centre (NCSC) says of BYOD that: 'balancing your organisation's need to protect and maintain control of its data and systems against the usability, and privacy expectations of the device owner can be difficult.'

They recommend that organisations take the zero trust approach of 'never trust, always verify.' This removes inherent trust in the network where every request for access is assessed based on an agreed policy. Every device and every person must meet with authentication, authorisation, and device status conditions before they can access corporate data, applications, platforms, or networks at any level.

To make this work, security and network teams must look at their system architecture holistically and plan for implementation. Zero trust is not a solution but an approach to security and it must be agreed in advance by at every level in the company so that it can become an inherent part of a broader technology strategy.

What else can be done to make data centres more sustainable?

David Watkins, solutions director, VIRTUS Data Centres

Organisations are taking an aggressive stance on climate change and committing to tackle their own environmental impact, and the data centre industry is no different. Today's data centre operators are expanding their use of renewable energy, harnessing innovative approaches to cooling, and employing other efficiency-enhancing methods to meet green ambitions and minimise their impact on the environment. But what else can data centre operators do to get ahead of the game on mandatory climate change and sustainability commitments?

A super-charged circular economy

The idea of a circular economy isn't new, but the 'maintain, refurbish, renew and recycle' model is likely to become even more prevalent in the future. The approach ensures that the data centre industry can achieve maximum efficiency in the use of finite resources, support the gradual transition to renewable resources, and ensure the recovery of the materials and products at the end of their useful life.

From committing to getting more life out of all materials in a data centre (maintaining equipment) to refurbishing hardware where possible, and recycling parts that cannot be reused, there are plenty of benefits to be had and it's likely we'll see many more providers adopt these principles. But establishing a circular economy isn't without its challenges - most pressingly that many data centre providers don't own the IT equipment they host – and so rely on their customers to take a lead in adopting the approach.

Accordingly, two key areas of priority are likely to emerge; firstly, a sustained effort from data centre providers to educate and encourage partners and customers to embrace the model. The savviest providers will commit to working with their customers to prioritise this approach, as well as lobbying hardware providers to prioritise the longevity, reusability and ultimately the safe disposal of equipment. Secondly, a move away from solely focusing on IT hardware and applying the same principles to the wider infrastructure of a facility – to encompass all the areas which data centre providers can control.

A holistic approach to sustainability

Data centre operators know that to achieve true sustainability they must embrace a holistic approach, for example adhering to BREEAM regulations which look at the entire lifespan of a building, from the concept and design to construction, operation, and maintenance.

Until now, companies have successfully tackled their Scope 1 emissions (those from owned or controlled sources) and Scope 2 emissions (indirect emissions from the generation of purchased electricity, steam, heating and cooling). However, a big focus from now will be tackling Scope 3 emissions, which include the indirect emissions that occur in a company's value chain such as business travel, purchased goods and services, waste disposal and even employee commuting.

By measuring Scope 3 emissions, data centre providers will be able to assess where the emission hotspots are, identify energy efficiency and cost reduction opportunities, and engage suppliers and assist them to implement sustainability initiatives.

It's a journey

The ability of data centre providers to harness renewable energy sources has been game-changing in the industry's pursuit of a greener future. Many providers now use 100% renewable energy from sources like hydro, wind and solar. Fortunately, renewable energy is now not only more affordable than fossil fuels but can also be more reliable.

Data centre providers have also been looking closely at fuel sources. The use of hydrotreated vegetable oil instead of diesel in generators has the potential to reduce carbon emissions by up to 90% as well as eliminate SO2 and reduce harmful NOx emissions.

Other innovation is ongoing, with developments in areas such as fuel cells continuing at a pace. While they aren't viable right now, if they can perform at scale, they might present a compelling option for future green data centre power.

A collaborative future

Whilst individual providers are working to become more efficient and make progress towards their green ambitions, ultimately, the industry must work together to solve its green challenges. From sharing best practice to setting up multi party task forces, there is plenty of scope for, and benefit to, more collaboration.

In parallel, data centre providers are encouraged to capitalise on funding available for green initiatives. As well as discreet research projects, there is more than £5 billion of funding available to help UK businesses become greener as part of the government's commitment to reach net zero emissions by 2050. Funding opportunities will be awarded to businesses investing in green technologies to increase energy efficiency and/or reduce carbon emissions. The savviest providers will take advantage of these schemes, not only addressing their own green ambitions, but driving broader innovation too. ■

Solving the legacy storage trap

An essential infrastructure for the modern enterprise, storage is one pillar of the foundation upon which all business is built. Why then are so many enterprises stubbornly staying with outdated legacy systems? Amy Saunders asks the experts

The legacy storage conundrum

Thousands of businesses around the world still rely on legacy systems for data storage. While admittedly robust, legacy storage can cause big productivity dips, data loss and unnecessary downtime.

Some of the classic frustrations, according to Sergei Serdyuk, VP of product management, NAKIVO, include hardware and software limitations; poor performance; lack of scalability; limited accessibility; and cost.

Tony Hollingsbee, SSD business manager, EMEA at Kingston Technology, agrees: "the major drawback to the continued use of legacy technologies is the loss of performance and even data, by comparison with the reliability, security and high performance of modern storage drives."

David Feller, vice president of product management and solutions engineering, Spectra Logic, meanwhile, says that the biggest frustration with legacy storage systems is compatibility with newer or more modern interfaces. "As more data centres leave fibre channel in favour of ethernet and SAS, storage devices need to follow suit to remain relevant. Likewise, as more and more organisations integrate cloud and cloud offerings, many legacy storage systems don't support an S3 interface and object storage," explains Feller.

Wes van den Berg, VP & GM, UK&I at Pure Storage, concurs that legacy architecture can't keep up with modern workflows and the exponential growth of unstructured data, hampering innovation efforts. "Legacy storage architectures like disk-based systems have become a significant burden for enterprises. They are expensive to run, difficult to manage, power-hungry, can take up large amounts of space, and can also be unreliable, causing disruption and risking the stability of valuable data," he says.

Indeed, legacy systems place a huge strain upon businesses in terms of skills, man-hours, and inefficiency. "While competitors are enjoying the agility, scalability, and accessibility of cloud-native solutions, maintaining your legacy system becomes harder and harder – and it's dependent on employees that don't benefit from it," says Tim Hood, VP for EMEA & APAC, Hyland.

Is it time then, to look to the future for a modern, flexible solution?

"Replacing mechanical HDDs with SATA SSDs in a computer and/or server can be a game changer in terms of performance, allowing shorter system booting and application loading times, resulting in a more satisfactory user experience," says Hollingsbee. "Transitioning to the latest generation of SSDs (PCIe NVMe), improves performance significantly, but due to the new interface and communication protocol on SSDS, this might require a bigger upfront investment in hardware."

Serdyuk, too, believes that advanced storage solutions offer greater reliability, scalability, cost-effectiveness, performance, and accessibility for modern-day businesses: "for example, software-defined storage (SDS) allows for more flexible and scalable storage management, while all-flash arrays (AFAs) can provide high-performance storage. Cloud storage solutions also offer cost-effective scalability and flexibility while reducing the need for on-premises storage hardware."

"Flash-based storage provides much higher speed and performance than legacy systems. Not only that, but flash is now available at a more economical price point than disk," concurs van den Berg. "In addition, its physical footprint is significantly smaller - enabling enterprises to reduce data centre floor space and cut power consumption. As unstructured data growth continues, the need for a modern platform to provide a more sustainable and scalable storage solution for everyday workloads is evident."

'Just upgrade your storage'

"It sounds so easy… just upgrade your storage," explains Feller. But when it comes down to it, "there are almost always larger forces at play," continues Feller. "How is the data migrated? Was it written in a proprietary format? What does it mean for general workflow? Will users be able to access the new storage in the same way? These are the things that keep businesses on legacy systems past their useful life."

Hood adds that, often, those operating legacy systems feel like they've hit an impasse. Removing a system that spans the entire business can feel like a seismic task – but failing to do so may allow competitors to accelerate away, and potentially alienate employees that had hoped for the ability to work remotely. "Similarly, you could risk discouraging new talent from joining – the majority of whom want to work for companies that utilise the latest technologies," he adds.

As a result, many businesses try to compromise between legacy system and modern iterations by forcing their existing solution into a cloud environment via a patchwork infrastructure of compatible platforms and integrations – 'cloud-enabled' rather than 'cloud-native.'

"This is a compromise: it compromises performance and business security, without properly solving the problems that the business faced in the beginning. Short-term fixes are seen as preferable to ripping off the metaphorical plaster, especially if creating stop-gap solutions is the norm," asserts Hood.

Despite their decreasing effectiveness, businesses may hold on to legacy storage solutions for a variety of reasons, including cost, lack of expertise, data migration complications, and the big one: fear of change.

"Some businesses may be hesitant to adopt new storage solutions due to concerns that it would disrupt their routine workflows," says Serdyuk. "This fear can be attributed to the learning curve associated with a new system or the possibility of unforeseen problems, such as compatibility issues. This can be particularly challenging for businesses that have been using their legacy systems for a long time and have become accustomed to them."

Indeed, typically legacy systems have been in place for many years and businesses worry that migrating existing data to a new solution will cause disruption, "but this doesn't have to be the case," says van den Berg. "The move to modern flash-based storage systems actually reduces the chance of disruption as it provides better performance, scalability and reliability. Additionally, the legacy approach of 'buy now; use for 3-5 years; then rip and replace' ties customers into solutions which may not be suitable. There's no flexibility in these legacy approaches and organisations should be demanding this from vendors so their needs are met, and they can scale up and down as needed."

The impact of digital transformation

Digital transformation efforts have rapidly increased the volume of data generated, and hybrid working has accelerated this further. Data created, captured, copied, and consumed worldwide is expected to reach 149Zb per year by 2024 - a 1,092% increase in the last decade.

"Such rapid data growth has significantly changed storage requirements; businesses need solutions that can cope with large volumes of unstructured data, scale easily and that can manage modern workflows," says van den Berg.

Digital transformation is "one of the biggest impacts we've seen on modern storage, and it's disappointing that more storage vendors haven't addressed it," comments Feller. "Data synchronisation becomes a big concern. There's little advantage to building storage silos in multiple places. Storage in a hybrid environment should offer synchronisation between cloud and on-prem repositories or between multiple cloud repositories."

Indeed, a successful hybrid workflow demands that data is accessible wherever it's stored. "We traditionally think of on-prem and in the cloud, but a multi-cloud workflow is also considered hybrid," says Feller. "We all know by now, it's a lot easier to put your data in the cloud than it is to get it out. Egress charges tend to be excessively higher than storage charges. Moving between clouds or pulling data back to an on-prem location isn't always financially viable. Storage for such situations must be able to address such issues as simple, free egress. Otherwise, we're setting up organisations for a return to vendor lock-in."

Hollingsbee agrees that with advancing and more sophisticated technologies, there is greater need for more accessible data. "The growth of data does not only exist in terms of volume but for cross-business need. A decade or so ago a lot of 'cold' storage would be stored on tape – but the advancement in data analysis means that companies are looking at historical data points and customer behaviours to give real insights in how they can gain a competitive edge and improve operations."

Does (enterprise) size matter?

Across all enterprise types and sizes, storage is a vital element of the business strategy. Adequate storage, from a capacity and performance perspective, is essential for providing reliable and responsive access to information.

"The bigger the company, the more data it is likely to generate and that means a greater demand for storage and archiving facilities," says Hollingsbee. "What the data is used for is also significant. We see organisations that utilise data across hundreds of applications even when they have a small head count. It comes down to data utilisation and what they are bringing to market."

Indeed, as organisations grow, they tend to generate and store more data, which can lead to a more complex IT infrastructure involving multiple storage systems, various applications, and numerous user devices.

"To meet these storage needs, enterprises must have enough capacity and better management of storage systems. The specific storage requirements vary across organisations, depending on their workload and priorities. For instance, some enterprises may need high-speed flash storage for real-time data processing, while others prioritise low latency for applications like high-frequency trading," explains Serdyuk. "Additionally, certain companies may prefer NAS or SAN solutions for specific tasks such as video editing."

van den Berg agrees that the larger an enterprise, the more data it will create, so bigger enterprises have more significant storage needs. "However, for all organisations, storage needs are increasing as data volume grows. Businesses need an infrastructure that can not only deliver in high-performance and low latency, but that can scale alongside them. That's why we're seeing the increasing popularity of subscription-based storage which provides businesses with the flexibility to easily scale up data storage as and when needed, while also delivering the performance and security of modern storage solutions."

Disagreeing with his fellow storage experts, Feller asserts that "quite frankly, it [size] doesn't [matter]. There are very small organisations that produce petabytes of data and very large organisations that aren't data intensive at all. It's the amount of data an organisation holds and the amount of time they hold it that really impacts storage needs." ■

Debating the modern network

With digital transformation in full swing and data volumes booming, how can network managers choose the right solution for their enterprise? Amy Saunders checks in with those in the know

Public networks have been around for decades and have transformed our lives as consumers. For enterprises, they are quick and inexpensive to deploy, with great bandwidth capabilities.

Public networks offer simplicity, explains Mike Kennett, head of regulatory affairs, Freshwave. "The network infrastructure already exists, so if there's coverage on site then the enterprise only needs to source devices and SIM cards. Use of public networks is infinitely scalable, so works for enterprises of all sizes."

"Public networks are convenient, and increasingly used by organisations that have made the shift to cloud services, meaning their focus is on obtaining fast and cost-effective internet connectivity," says Richard Parkinson, director, FarrPoint.

However, the main focus for MNOs is consumer services, which is not always consistent with enterprise needs. Public network coverage and capacity is often poor in workplaces, especially in buildings constructed using modern energy-efficient materials. Additionally, the type of service needed by an enterprise may be very different from that for a consumer.

"Consumer services such as video streaming use mostly downlink traffic; consequently, public networks are designed to provide greater downlink data rates," outlines Kennett. "Conversely, enterprises using other types of devices, such as wireless CCTV or mobile cameras on robots, are likely to need more uplink capacity than downlink. In addition, some of the advanced features of 5G designed for industrial applications, including ultra-reliable low-latency communications (URLLC) and massive Machine Type Communications (mMTC), will not be available on public networks for some time."

Trusting in the network

Among some organisations, the lack of control over the network, and the fact that it isn't customisable, is a real sticking point. The enterprise has reduced control over security measures, meaning the public network providers hold all the cards.

As such, private networks have emerged in the last few years to offer exciting opportunities for organisations like control, flexibility, scalability, increased security, and no monthly fees.

One major difference between private and public networks is that there is no SLA in place for the latter - if the network goes down, there is no commitment from the provider. "You're in their hands and their timeline for when it will be up and running again," says Justin Day, CEO of Cloud Gatweway.

"Organisations that still host the majority of their services and applications on-premise may still need the guaranteed quality of service, availability and security of a private network," agrees Parkinson.

Private networks give assured connectivity with dedicated resources and spectrum. "And they're highly customisable as they are tailored to the exact needs of the organisation," adds Kennett. "Private networks are therefore likely to be a better choice for mission critical use cases, and for requirements which can't currently be met by MNO networks such as URLLC. The disadvantage is the cost of additional infrastructure, although hardware and software costs are reducing as more vendors enter the market."

Indeed, the up-front costs can render private networks uneconomic for some enterprises, plus there is the maintenance support, and associated staffing, to consider.

Hybrid networks have thus emerged as a means for enterprises to get the best of both worlds. Users share some parts of the infrastructure to help reduce costs, gain greater resilience, and achieve increased capacity from aggregating two networks.

Catherine Doherty, enterprise networking leader, Cisco UK&I, says that the hybrid network model is becoming "the norm" for many enterprises today. "Our '2022 Global Hybrid Cloud Trends Report' shows decision-makers are moving to hybrid networks for better business agility and access to cloud-based services," says Doherty. "However, running a hybrid environment comes with security challenges and increased operational complexity."

Managing big data

With digital transformation well and truly upon us, data generation is expanding exponentially, putting significant strain on networks.

"As IoT devices grow from billions to trillions, demand for bandwidth grows not only from connecting devices to the network but also from the AI/ML workloads required to drive insights from IoT," says Doherty. "Applications such as generative AI, search, language processing, and recommendation engines, require more bandwidth than traditional workloads. Organisations will need to adapt their networking strategy to enhance and extend their capabilities to meet new competitive challenges."

So, what does that mean when it comes to deciding between public vs private vs hybrid networks?

Much of the new data traffic is uplink in direction, in contrast with consumer phones where the traffic is overwhelmingly downlink. "So private networks, with their uplink/downlink flexibility, might be the best choice for organisations generating large quantities of data from wireless devices," says Kennett. "5G is also likely to be a better technology option than 4G due to its faster data rates. A private network allows an enterprise to utilise 5G technology even if there's no public 5G network coverage at the site."

The data composition represents a significant component in choosing the right network. "For enterprises moving content that they don't mind being in the public domain, public internet is the way to go," explains Day. However, for important or private data, "it's possibly better to look at a private network."

"An organisation will need to have clear IT priorities to select the right enterprise network," says Doherty. "Whether your priority is gaining 360-degree network visibility or security, or simplifying your wired and wireless access, branch, or WAN networks with software-defined networking. The right enterprise network architecture can optimise access to cloud applications, a mobile workforce, and/or IoT connectivity. These architectures adapted to your priorities can scale from the smallest to the largest deployments."

According to Day, "there isn't a single right answer. Some services are better suited to private networks, others public, and there are some that will benefit from multiple connectivity technologies. It's all about weighing up responsibility versus control, cost, and performance - and how much you need of each." ■

IoT security solutions for enterprises

With the number of connected devices set to boom over the next decade, security has become paramount for the smooth operation of IoT networks the world over, says Dennis Mattoon, chair of DICE Work Group, TCG.

According to Statista, the total number of connected IoT devices used worldwide is projected to reach over 30 billion units by 2025, a significant growth compared to the 13.8 billion devices being deployed in 2021. Enterprises looking to leverage this technology within their operations must follow the latest guidance and security solutions available to ensure their systems are sufficiently protected against the new wave of threats on the horizon.

Establishing 'trusted computing' with a TPM

Failure to deal with these threats can lead to significant consequences for enterprises. The 2016 Mirai botnet attack used thousands of compromised devices to cause a worldwide internet blackout for a number of organizations. At its peak it targeted over 600,000 vulnerable IoT devices, whilst disrupting more than 900,000 Deutsche Telekom customers in Germany and almost 2,400 TalkTalk routers in the UK. Mirai was a type of malware that infected and conscripted IoT devices into a centrally controlled group called a 'botnet.' This is just one type of cyber-attack that occurs on a regular basis that enterprises need to be aware of.

The first port of call for enterprises must therefore be to utilize a Trusted Platform Module (TPM) within all applicable devices. A TPM can be scaled to different platform types, depending on the device's specific requirements. Enterprises adopting this technology will be able to protect, detect, attest and recover from any malicious behaviour by incorporating a 'trusted computing' approach to security. Any data will be signed and verified to ensure it has come from a reliable source and that the information is accurate. Hardened storage for software or platform keys is also provided to protect and attest any algorithms used within an enterprises' model.

Network equipment is the lifeblood of enterprise operations, and is required to combine, split, boost, or segment information across the ecosystem. This will include any switches, routers, gateways, or firewalls found in a system. The most critical aspect for these elements is to protect the private key integral to its identity. Deploying solutions such as the TPM 2.0 can help to create a strong and durable identity assigned to new devices during the manufacturing process. This identity, known as IDevID, applies to a wide range of critical functions such as zero touch configuration, and enables a secure deployment at scale. As a result, cyber attacks will not be able to mimic or impersonate the devices found within an enterprise's ecosystem, meaning operations can trust the devices they utilize.

Ensuring integrity through DICE

The TPM is a vital tool that enterprises can use to ensure the integrity of a device, yet the fact remains that many devices prevalent within an enterprise's ecosystem will not contain one.

To establish a strong line of defence within these devices, Device Identifier Composition Engine (DICE) specifications should be adopted. This provides a guide to establish trust within all systems and components, regardless of whether a TPM is incorporated. Through DICE, devices can integrate a cryptographically strong identity, assist in safely deploying and verifying software updates an enterprise may require, all whilst verifying and attesting any information received from a device.

Staying up to date with the latest standards available is paramount to strong device security, and the latest DICE specification allows devices within an ecosystem to perform measurements and produce claims required in evidence, all at near zero cost. This makes it a cost-effective solution for enterprises to utilize. All aspects of the attestation process are covered, meaning enterprises leveraging this solution can trust the device to do its job without any fear it's been tampered with.

A proactive approach to security

Root-of-trust hardware like DICE helps enterprises establish integrity and accuracy within connected devices, but for smaller devices found within operations (such as sensors), an enterprise may choose to implement something akin to the Measurement and Attestation Roots (MARS) specifications.

Through MARS or similar solutions, an isolated pair of hardware root-of-trusts are integrated into IoT devices to implement logic directly into the hardware while remaining separate from the micro-compressor environment, increasing the overall level of security. Solutions like MARS and DICE offer a premium security service at low cost, and therefore these should be an essential component in an enterprise's security make-up. ■

Scottish FRS moves to SD-WAN for future-proof services

The Scottish Fire & Rescue Service (SFRS) is the world's fourth largest fire and rescue service. SFRS front-line services are delivered locally from three strategically positioned hubs based in the North, West and East of the country. In addition to fire control and prevention, SFRS responds to many different emergency incidents including road traffic collisions, rope rescue, water rescue, hazardous materials, and flooding as well as assisting partner agencies in keeping communities safe.

In March 2021, following a competitive tender, SFRS awarded MLL Telecom (MLL) an initial four-year Wide Area Network (WAN) services contract to replace their existing nationwide IPVPN-based WAN procured in 2016 and the provision of ongoing fully managed WAN services.

Following a period of extensive planning, MLL commenced the transformation programme in October 2021. This was completed successfully and on time in December 2022.

Project requirements

SFRS required a single network supplier capable of delivering and managing a future-proofed WAN solution to connect over 360 fire and rescue stations throughout Scotland, including highland and island areas. This had to ensure an enhanced user experience through reduced network latency - especially at remote sites – and support SFRS's planned migration to public and private cloud-based services.

MLL proposed a managed SD-WAN solution based on Fortinet technology, enabling connectivity to all SFRS sites irrespective of their location or underlying connectivity technology. SD-WAN allows bandwidth to be aggregated over multiple circuits – especially important for some of SFRS's remote locations that are very poorly served with connectivity. The solution also supported SFRS's planned move to the cloud while ensuring the existing elevated levels of security and control would be maintained.

Moreover, detailed single pane of glass reporting shows how the network and applications are performing. Security is also fully integrated through the highly regarded Fortinet SD-WAN security fabric.

Overcoming challenges

The WAN project required migrating multiple sites nationwide, however, the network technology infrastructure differed considerably. While the larger SFRS fire stations and offices located in and around metro areas benefited from fibre connections including FTTP, many of the sites in rural and remote locations used a hybrid technology approach comprising Superfast, 4G and DSL technologies. Adding further complexity, several sites in Glasgow utilised a microwave network.

The sheer remoteness and rugged environment of many of the SFRS locations, ranging across all the Highlands and Islands, presents an engineering challenge. This adversely impacted the performance of the previous WAN solution, sometimes preventing routine tasks undertaken by SFRS personnel, as well as more critical ones such as accessing cloud-based training applications.

Furthermore, ferries and planes were prone to cancellation at short notice due to the often unfavourable and highly changeable weather conditions, causing delays in equipment delivery and field engineering. Comprehensive and flexible coordination and route planning was therefore of paramount importance.

"The large number of sites involved, often in remote locations, combined with the considerable distances involved and changeable weather all contributed to making this a challenging but very satisfying project," said MLL field engineer Thomas Guild. "MLL's super-efficient coordination support made all the difference. It was vital that parts and engineers arrived on time, which they did, no matter how remote the location. On more than one occasion our travel plans had to be changed at short notice due to severe weather. One time, I recall receiving a message from our project management team to abort just as the plane was preparing for take-off to Fair Isle – they had seen a hurricane was forecast to hit the area within the next 48 hours which would have seriously delayed my return and ongoing implementation schedule!"

Project delivery and outcome

A major factor in the project's success was the close working relationship that has been forged between MLL and SFRS. This ensured that the migration was seamless to end-users and that the network service continued, uninterrupted in-spite of a change in suppliers.

At the outset, MLL assigned an experienced senior project manager to lead the programme and establish a robust transition plan. This included liaison with SFRS's Project Lead with regular progress meetings, enabling open and transparent communications.

A phased approach to transitioning SFRS sites to the new SD-WAN was agreed. MLL's technical design architect worked with both SFRS and the previous supplier's technical teams to agree the technical migration process as well as detailed testing and acceptance plans. MLL's network operations centre (NOC) engineers also met with SFRS's IT team to gain additional insight into the existing network.

Site migration was undertaken by MLL's field engineering team. They were responsible for visiting the sites, testing the lines, and configuring them to support the SD-WAN. Between October 2021 and April 2022, MLL's field engineers undertook continuous travel five-days a week with overnight stopovers in local hotels and lodgings. Ferries or planes were used to reach the more remote destinations including Orkney, Fair Isle, Shetland, and the Hebrides. In total the team accumulated over 30,000 road miles by the time the transformation project completed.

"MLL has provided SFRS with a reliable, cost-effective, flexible and future-proof WAN solution, supporting our ongoing digital transformation and vision," said Sandra Fox, head of ICT, Scottish Fire and Rescue Service. "MLL's SD-WAN and engineering services ensure we can continue to depend on resilient high-quality voice and data services while also paving the way for a smooth transition to a cloud-based architecture over the coming years." ■

Upgrading legacy systems for Avon FRS

Operating across 134,753 hectares and responsible for keeping more than one million people safe, Avon Fire and Rescue Service (FRS) provides emergency and protection services to the communities of Bath and Northeast Somerset, Bristol, North Somerset, and South Gloucestershire.

Headquartered in Portishead and with 21 fire stations across the area, Avon FRS's 500 Wholetime firefighters, 120 on-call firefighters, 35 control room personnel and 120 support staff, responded to over 9,000 incidents in 2021.

Replacing legacy systems

Many secondary bearers used as back-up networks for station end mobilisation systems in fire stations across the UK are rapidly approaching end-of-life and need upgrading and replacing. PSTN is scheduled to be retired in 2025 and mobile operators have announced the phased withdrawal of 3G and 2G networks from this year.

The legacy Paknet service that Avon FRS was using for its secondary bearer – the back-up network connecting the station end to the control room – was scheduled to be withdrawn at the end of March 2022. Avon FRS needed an alternative solution as a back-up in addition to its primary bearer of a wired WAN link, to ensure continuity of service for its station end solution.

In addition, the fire coders – the core hardware technology that mobilise crews – needed to be upgraded as they approached end-of-life. The coders receive information from the control room, via the primary bearer (or secondary bearer if there is an issue with the primary bearer) to operate multiple devices to directly mobilise resources in the fire station.

The equipment activated by the fire coders includes printers in the station and mobile data terminals in the fire appliances, both receiving critical information about the incident. A wide range of other devices are also activated in the fire station to mobilise crews, including radio paging for retained stations and control relays to flashlights, open doors and turn off cookers. It was therefore essential that Avon FRS remained connected via a replacement system for Paknet and was utilising the most up-to-date, supported, and secure operating systems.

"We are delighted with our collaboration with Telent to upgrade and replace our legacy technology for our mission-critical station end communications in readiness for the transition to ESN," said John Craig, station manager at Avon Fire and Rescue Service. "Working with Telent has provided us with the complete confidence that our firefighters have access to unfailing and continuous communications to effectively and diligently undertake their daily duties."

Meeting rural and urban needs

To upgrade its station end solution, Avon FRS employed Telent to deliver a cost-effective solution to upgrade the operating system in the fire coder and implement a new solution for its secondary bearer.

This was the first deployment of its kind and replaced Paknet with a router solution that terminated the primary bearer and provided a secondary back-up bearer using a mobile network data service for over-the-air connectivity. The router is equipped with a multi network SIM. This allows the most appropriate mobile service provider to be automatically selected for the back-up bearer removing any issues of mobile service coverage which is particularly important for rural and remote based stations.

Telent provided comprehensive design, testing and deployment services. This started with initial development and pilot testing of the solution in its specialised lab followed by prestaging all equipment to minimise time on site and maximise quality of service for the main project deployment. The pre-staging of equipment in Telent's secure facilities included testing and fully configuring all equipment to reduce any early-life failures and associated on-site engineering visits.

"Telent offers an end-to-end integrated upgrade route for fire and rescue services across the UK," said Barry Zielinski, operations and services director at Telent. "Our 4G-enabled ESN-approved technology is the perfect solution to replace existing systems that are imminent for retirement, and our fully managed service has ensured a seamless transition for Avon Fire and Rescue Service in preparation for ESN. Telent is the partner of choice for emergency services organisations looking to work alongside a company with the knowledge, expertise and vision to innovate services in the years ahead."

Prepared for the ESN transition

The new solution has provided Avon FRS with improved resiliency and security and delivered an alternative back-up bearer to replace its legacy Paknet network to ensure its fire stations remain connected even if the main network goes down. Avon FRS now has a solution that ensures business continuity through its upgrades to the fire coders and the new router solution that is compatible with the ESN Connect service, providing readiness for the nationwide transition to ESN.

The new router solution is equipped with a cloud management application that provides secure remote monitoring that can be conducted on behalf of the customer. Telent can administer new change configurations centrally and across all of Avon's 21 stations via the secure cloud platform. The cloud management solution also has the ability to directly monitor and alert Telent's network operations centre should any issues be detected.

The system upgrade and end-to-end replacement of the legacy back-up network provides critical station end communications to Avon FRS. Importantly, the network refresh supported Avon FRS' station end systems and prepared the organisation's mobilisation solution for ESN compatibility. ■

Communication fit for a King

Halo Solutions played a crucial supporting role in keeping the public safe during 'Operation Golden Orb,' the counterterrorism and security plan devised by the Metropolitan Police for the Coronation of King Charles III and the Coronation concert at Windsor Castle.

The Coronation was the UK's largest state event since the Queen's funeral. Operation Golden Orb was also the single biggest security and policing operation that the Metropolitan Police had mounted in recent years, with more than 11,500 police officers and staff protecting 312 of the world's leaders and visiting dignitaries. The Metropolitan Police worked with multiple agency partners including British Transport Police, London Fire Brigade and London Ambulance Service, with support from other police forces across the UK.

There are many challenging parts to protecting the public at events like the Coronation, explains Lloyd Major, founder, and CEO of Halo Solutions.

"Top of the list will always be protection of life. That can mean taking account of threats such as vehicles used a weapon, IEDs, marauding attackers, as well as the physical space the crowd has to gather and the numbers of people attending," says Major. "Can they get in, assemble, and get out safely? Move freely, access the facilities they need for their comfort and wellbeing? On top of this, where large crowds gather, the cellular network can struggle for capacity/bandwidth and any systems like POC radios or mobile apps designed for public safety or work use by the contractors can struggle."

Accordingly, the Halo (v5) system - a serverless, cloud-based SaaS platform that deploys right to the edge of the network, powered, and supported by AWS - was utilised to monitor and protect critical infrastructure and transport links during the Coronation. It was deployed to monitor crowd ingress and egress through places like Waterloo and Windsor train stations, with primary functions including crowd safety, incident management, monitoring of security personnel and assets, and implementation of counterterrorism prevention strategies, monitoring for suspicious persons, packages, vehicles, and baggage.

It follows the announcement by Metropolitan Police commissioner Sir Mark Rowley that his officers had to target a "criminal network" during the Coronation, which included people posing as fake security stewards, who were caught with bottles of paint that they intended to throw at the parade. Further intelligence indicated that the group planned to also use rape alarms and loud hailers to disrupt the Coronation and vandalise monuments with paint.

The Halo System acted as a central command and control function monitoring multiple feeds of security information through the Coronation weekend from several sources at the two key train stations and the surrounding infrastructure at both locations. Several suspicious incidents and individuals were identified, monitored, and reported.

"We were delighted and honoured to have played a small but important role, working with our partner agencies and clients to help maintain public and crowd safety for the Coronation at key locations and surrounding infrastructure with an estimated 20,000 people travelling to Windsor to attend the Coronation concert and many more in central London. This was an incredibly well organised event by the Metropolitan Police and huge credit to all the security companies and partner agencies involved, pulling this off with little to no incident whilst the eyes of the world were upon us," says Major. "Security and crowd safety of the public at major events has never been more important following the disasters of Hillsborough and more recently, the Manchester Arena bombing of the Ariana Grande concert, Astroworld, Itaewon crush deaths and the o2 Brixton Academy fatalities."

The Halo (v5) system provides a wide range of risk mitigation services in crowd and public safety. It provides a unique command and control of major events with one core aim of safety and protecting the public. It provides incident management, crowd dynamics, heat-mapping, density, flow, and sentiment, as well as bodycam video, CCTV and drone footage integration, ticket scanning, security staff authorisation and public reporting for suspicious activity or packages as well as many other features.

The tech platform is also playing a significant role in major event security and crowd safety at music, sporting and live events at arenas, stadiums, and festivals, following the aftermath of the Manchester Arena bombing. With 'Martyn's Law' being introduced this year – which the government plans to introduce to all venues and stadia to ensure stronger protections against terrorism in public places – this will mean even greater responsibilities for venue owners, arenas, and stadiums, with mandatory checks and protocols.

"The Halo (v5) tech was designed to play a critical role in mitigating risks attached to major events before they happen, with a focus on prevention. In the unlikely event those risks do escalate, Halo (v5) effectively and rapidly brings together all the different security, health and safety systems, medical teams and partner agencies involved in an event under one command and control system," adds Major. ■

How UCaaS can power the modern-day workforce

Ross Slogrove, UK & Ireland country manager, Ringover

The workplace today looks quite different from how it was before the pandemic. That's because many workplaces do not have their employees working full time from their desks. Instead, they are dispersed between the office, their home and other feasible working locations. Research shows that hybrid working has retained its popularity post-pandemic, with 68% favouring this model, according to a study from Slack based on 10,000 desk workers across six countries.

Of course, this has only been made possible with the help of communication and collaboration tools such as Zoom, Teams and other cloud-based calling technologies. Prior to this, these technologies were rarely talked about. Now, businesses cannot succeed without them. In fact, at the end of 2022, Microsoft announced that Teams was now being used by 270 million users worldwide.

Unification equals collaboration

Technology is proving essential for businesses, who without it, may struggle to keep pace with competition and meet the expectations of modern-day consumers.

Collaboration tools are beneficial in their own right, but, to really enhance the true potential of these tools, businesses must unify their solutions for the following reasons.

Unifying all business communication tools allows for more efficient communication across teams, departments, and locations — especially important considering the proportion of people working under a hybrid model. This ensures that everyone is on the same page, no matter their location or device, which improves coordination, information sharing, and faster decision-making.

By centralising all collaboration tools, businesses can provide their employees with an interface that's easier to use and saves time switching between multiple tools while working on a project. This also enables employees working outside of the office to access the software they need to complete their jobs without any disruption. This leads to increased efficiency, as businesses can reduce the number of applications they are using, which can help in lowering the cost of software licensing, maintenance, and support.

Making the right choice

So, how do businesses unify their comms tools? While there are many collaboration tools on the market, a one-does-all solution, such as a unified communications (UC) platform, is one of the best investments a business can make.

UC unifies numerous business communication tools, including services like voice, video conferencing and instant messaging. The system enables these forms of communication to work together in one unified environment, allowing the user to stay in touch at any time using any device. Ultimately, the goal of UC is always to make work easier by eliminating the need for multiple platforms, introducing portability, and simplifying communication.

But how do businesses determine what platform is best for them? Firstly, identifying the business' needs and what it wants to achieve from using a UC platform will help pinpoint what type of platform is best. For instance, what is the budget? How many people from the business need access to the platform? What will they be using it for?

Other ways to distinguish which UC platform is most suited to your business is to consider the potential for scalability — think how your business will look in five years' time, and what you'll need to support future needs, not just the here-and-now. Security must also be acknowledged for any business in today's increasingly cyber aware world. This involves understanding whether the platform offers end-to-end encryption and firewall security, otherwise there could be additional costs to consider if security is breached.

However, with productivity being undeniably one of the most significant benefits of using a UC platform and to reap the benefits of this, businesses should look out for the software's ability to integrate with CRMs and help desk tools. Whether your business uses industry favourites such as HubSpot or Salesforce, or it relies on the capabilities of Bulhorn to support recruitment, or PipeDrive for sales, having a UC platform that integrates with CRMs, boasts significant benefits as it bridges the gaps between the tools and their interfaces, without the need to download multiple applications.

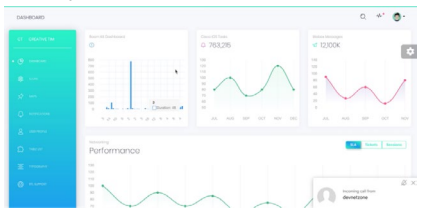
The pandemic has ushered in new workforce trends that are continuing to shape the way businesses work. As a result, businesses have relied on collaboration tools to stay in touch with employees, regardless of where they are located. But UC takes the capabilities of these collaborative tools to the next level by helping to build a more agile, productive, and connected workforce that performs efficiently in the modern-day hybrid workplace. ■

PRODUCTS

Cisco Webex is a cloud-based collaboration platform that provides a comprehensive set of tools to enable teams to work together from anywhere.

A great solution for online meetings, real-time messaging and file sharing, and whiteboarding, Webex provides secure and reliable communication solutions for businesses of all sizes, from small startups to large enterprises.

Webex allows users to host video meetings with up to 100 participants, with features such as screen sharing, whiteboarding, breakout rooms and file sharing. Another feature is audio conferencing - Webex provides VoIP audio conferencing services, allowing up to 1,000 participants onto a single call. Meanwhile, webinar capabilities allow presenters to share slides, videos, and other content with large virtual audiences. The solution also includes tools for virtual training include live chat, polling, and reporting capabilities. Webex integrates with popular applications such as Salesforce and Slack and Cisco's own unified communications platform. Finally, various security features protect users' privacy, including end-to-end encryption, password protection and identity verification.

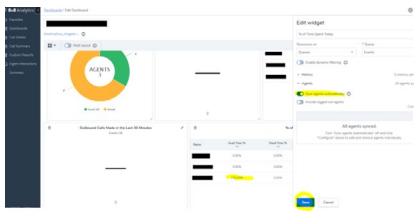


8×8 eXperience is a comprehensive cloud communications and contact centre platform designed to help businesses improve customer service and collaboration. It offers features such as unified communications, a contact centre, video conferencing, analytics, and AI.

Built on a single, secure platform and providing a unified experience across voice, video, chat, and team collaboration, 8×8 eXperience delivers powerful insights into customer behaviour and agent performance, enabling businesses to make smarter decisions. Indeed, 8×8 eXperience is designed to help businesses increase customer satisfaction, reduce operational costs and drive growth.

Features include a virtual VoIP phone system that can be integrated with existing phone lines or used as a stand-alone system; video conferencing with up to 500 participants in HD quality and features like screen sharing and recording; chat and collaboration that can be integrated with email, calendars and other applications, offering features such as group chat and file sharing; cloud storage; contact centre with features like call routing, customer analytics and reporting; a comprehensive set of application programming interfaces to integrate communications systems with other applications, such as customer relationship management systems.

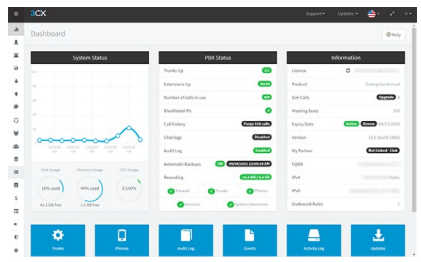
8×8 eXperience is also compliant with industry standards such as HIPAA, GDPR, FISMA and Privacy Shield, and offers features such as encryption and two-factor authentication.



The **3CX** unified communications solution is an open-standard, software-based IP private branch exchange that works with popular IP phones, Session Initiation Protocol trunks and VoIP providers to provide a full PBX solution. This approach to PBX comes without the inflated cost and management headaches of a traditional PBX.

3CX provides unified communications features such as video conferencing, web conferencing, presence, chat, softphones and webRTC. 3CX also offers a mobile app for iOS and Android, allowing users to make and receive calls, schedule conferences, have video calls and chat all from their mobile devices.

The unified communications platform integrates the features of a modern business telephone system with VoIP, video conferencing, instant messaging, presence, and CRM; mobile apps are available for iOS and Android, allowing users to make and receive calls and manage their contacts from mobile devices. 3CX offers web conferencing solutions with screen sharing, video conferencing and audio conferencing, and provides auto attendants, which allow incoming calls to be automatically answered and routed to the correct person or department. Integration with popular accounting systems, ERP and CRM tools allows users to access customer information while on the phone and quickly respond to customer inquiries. Moreover, 3CX includes call recording and advanced call reporting which allows managers to track call volumes and durations while analysing other call trends.

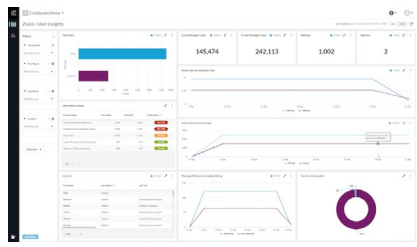


IR Collaborate is a unified communications monitoring solution that helps businesses predict disruptions and optimise performance across on-premise, cloud, or hybrid audio, voice, and other collaboration systems.

With IR Collaborate, managers can quickly identify root causes for issues, minimise user impact and diagnose problems using granular data analysis and historical information.

IR Collaborate allows enterprises to gain insights into system performance across network routers or layers and session controllers. Enterprises can monitor, respond to, or resolve issues in real-time and improve IT processes by troubleshooting multi-vendor unified communications from within a unified system. It also supports various platforms such as Microsoft Teams, Skype for Business, Zoom, Avaya, Polycom, Oracle, Ribbon, and more.

IR Collaborate enables businesses to ensure enhanced return on investment (ROI) by improving end-user experiences and organisational productivity. Enterprises can also monitor unified communication environments for meetings, calls, and interactions across applications, vendors, network paths, and elements.



The **Microsoft Teams** collaboration platform combines workplace chat, video meetings, file storage and application integration, enabling teams to collaborate and communicate securely in an organised way from desktop and mobile devices, both in office and from home.

Teams features a persistent chat functionality, allowing users to send messages, share files and collaborate in real-time. It also offers audio and video calling, integrated applications, task management, and polls and surveys. With Teams, users can access and share files across the organization, work on projects and tasks together in real time, and quickly find relevant information and conversations.

Microsoft Teams allows users to host virtual meetings with over 200 people, either through video or audio conference. Users can chat and collaborate in real time, with features such as threaded conversations, @mentions, and group chat options, as well as store and share files with other team members. Teams also integrates with OneDrive and SharePoint, making it easy to access and share files. The solution allows users to create tasks, assign them to team members and track their progress.

Please meet...

Jonathon Sharp, CEO, Britannic

Who was your hero when you were growing up?

My dad, amongst other things he was the regional director of Institute of Management. He has always challenged me and supported me in equal measure. He has been a great role model, showing me the value of hard work and been a great mentor and sounding board for me throughout my career. I was fortunate that my parents always encouraged me to try new things and not be afraid to fail!

Dad arranged varied work experience for me, including a work placement with a Midlands manufacturing business. The business had reached an impasse in introducing a new computer system despite having their best people on the job, because the computer outputs weren't matching the paper-based system. My challenge for the week was to solve this problem for the MD! I spent the first day with my head in my hands not knowing where to start and how I could possibly succeed where others had failed. That night my dad enquiring about my day and hearing of my reaction, taught me one massive lesson. There is no such thing as can't! He encouraged me to think laterally and logically, break down the problem and go back the next day and have a proper go with a clear mind and fresh perspective! On day two I saw the pattern and on day three I presented the results to the MD.

The lessons – step back, approach the problem calmly and remain positive. Test and review. All problems are solvable – it's all about mindset.

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

Like many people I did not really have a sense of what I wanted to do in my future career. I had always been interested in business and sales (from the age of 10!). When I left the sixth form, I stumbled into an interesting degree, Industrial Information Technology, which was in its first year being offered. I could not have selected a better degree to set me up for the workplace and industry that I work in today. This coupled with the early insights into the telecoms market, by attending a BT event at the age of 14 which piqued my interest in the industry set me in good stead for the future. Dad had worked at BT as an apprentice from the age of 16 right through to senior management at the age of 50, so I guess it was always in my blood!

The Rolling Stones or the Beatles?

Tough choice! If pushed I would have to say the Beatles, due to their rapid global success and impact they had at the time, the popularity and awareness of their music, slightly edging the Rolling Stones for breaking the mould and their longevity as a band. Either way both are fantastic examples of the impact and success of the British music industry.

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

I love working in IT and technology as it's so faced moving, with lots of new ideas to explore and value to create for the customers we work with. But if I had to be in a different industry then I would be an architect as I am passionate about trying new things, solving problems, creativity and design.

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

No such word as can't, always give it a go, do your best and be open to continue to learn and develop.

What was your big career break?

When I joined Britannic in 1997 and Richard Dendle, founder of Britannic, taught me the importance of adding value and customer service and gave me opportunities throughout my years in the business and the room to grow, constantly expanding my skills and knowledge.

Where would you live if money was no object?

I am fortunate to live in the heart of the South Downs National Park, close to the coast, with great countryside on our doorstep, access to amazing walks and scenery, good friends close by and a wonderful local pub. I think sometimes we underestimate the UK, with different seasons, wildlife, diversity of culture, our heritage and so many places to explore! Why would I want to live anywhere else?!

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

I'm going to choose three people:

Sir David Attenborough to wonder at his insights into the natural world.

Winston Churchill to understand how he overcame great adversity as our war time leader.

Leonardo Da Vinci, what an amazing all-rounder. He was a scientist, artist, architect, inventor, and engineer - you would not be short of topics for conversation!

What's the greatest technological advancement in your lifetime?

Until recently I would have said the iPhone, but I think advances and opportunity with Generative AI have the potential for a true paradigm shift! ■