



IN DEPTH:  
AI in data centres  
P8-10

## VR training: the new normal?

What businesses can learn from the military

Pat O'Connor, VRAI, p7



## Breaking the energy curve

How 5G is helping to increase efficiency

Tu Jiashun, ZTE, p13



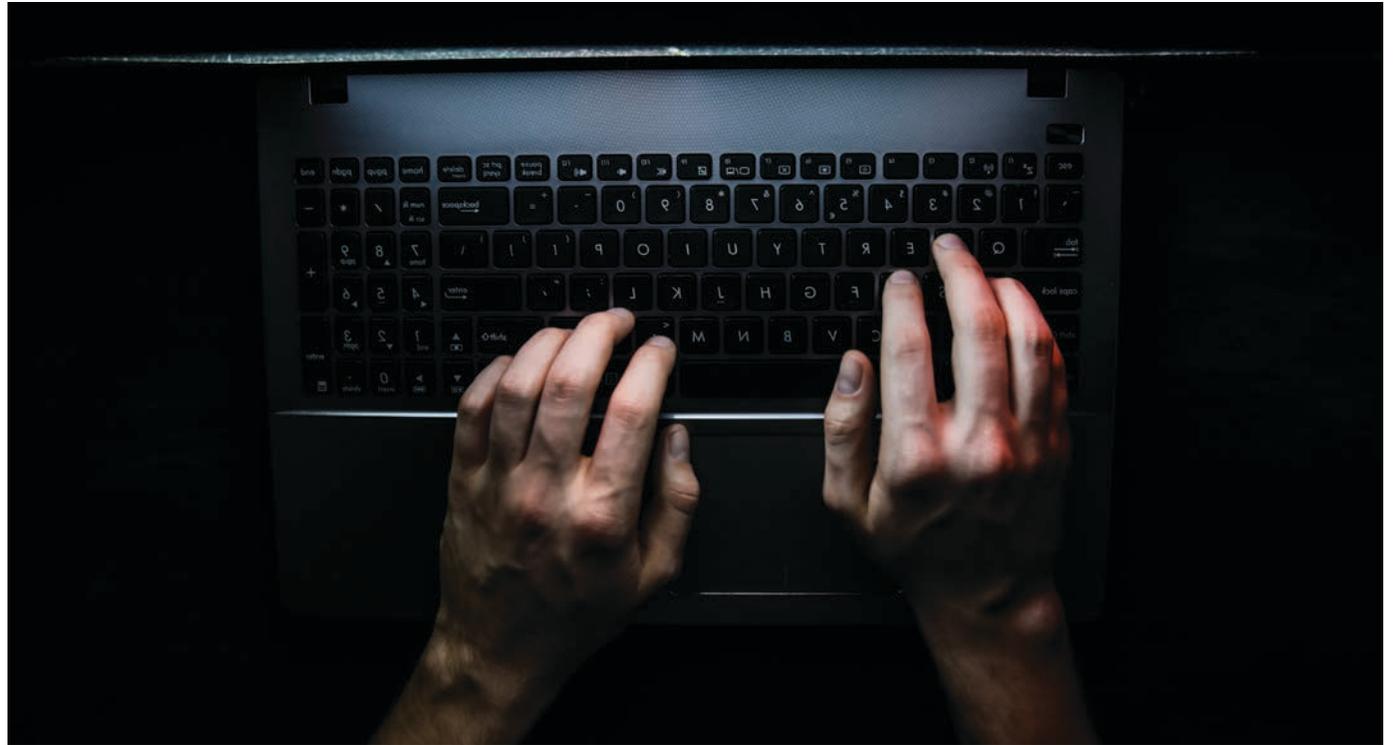
## Please meet...

Networking+ sits down with the Zivver CEO

Rick Goud, Zivver, p15



# Blackbaud hack leaves UK institutions exposed



**Cybercriminals obtained data belonging to universities, charities and other UK institutions following a ransomware attack on US cloud computing provider Blackbaud.**

The South Carolina-based firm was held to ransom by hackers in May and paid an undisclosed ransom to cyber-criminals. However, the world's largest provider of education administration, fundraising and financial management software did not reveal the scale of the breach.

Blackbaud has also been criticised after taking weeks to warn victims that data had been stolen.

In some cases, the personal details were limited to those of ex-students, who had been asked to financially support the establishments from which they had graduated. However, in other cases, it extended to staff, existing students and other supporters.

Some of the universities confirmed to have been affected include University of Birmingham, De Montfort University, Oxford Brookes University and University College, Oxford. The UK's National Trust as well as homeless charities The Wallich and Crisis, the terminal illness charity Sue Ryder, as well as the mental health group

Young Minds also make up the growing list.

However, the hack has not been limited to universities and charities. Some schools have also been affected, including St Albans in Hertfordshire, Radley College in Abingdon and St Aloysius in Glasgow.

ACS International, commonly known as "the American School" in London and Surrey also said there was a low-threat to its "alumni's and friends' information".

In addition, Maccabi GB – an organisation that provides services to 44 Jewish primary and secondary schools – said its data was among the compromised.

All the institutions that were affected are sending letters and emails apologising to those on the compromised databases.

In some cases, the stolen data included phone numbers, donation history and events attended. However, credit card and other payment details do not appear to have been exposed.

Andrea Babbs, head of sales UK and Ireland at security solutions vendor Vipre told *Networking+* that the Blackbaud ransom attack demonstrates the importance of a layered

approach to IT security and more specifically, powerful email security both in SMEs and larger organisations. "The consequences of Blackbaud deciding to pay out a ransom to protect sensitive data highlights the threat and damage that can be caused by not having the correct IT security infrastructure in place," she said. "With numerous universities and charities affected by the Blackbaud attack, the fact that personal details such as customer names and contact information was compromised and held to ransom by cybercriminals, showcases that even highly regulated industries can have vulnerabilities in their security processes. As with all data breaches, students, staff and supporters could now be left wondering how they can trust their educational facilities with personal information in the aftermath of this data protection failure."

Blackbaud insisted that "the majority of our customers were not part of this incident". It said in a statement that once the hackers had been paid, they had given "confirmation that the copy [of data] they removed had been destroyed."

*continued on page 2*

EcoStruxure  
Innovation At Every Level

Deploy Edge with  
**CERTAINTY**  
with EcoStruxure Micro Data Centre from Schneider Electric\*

SmartUPS<sup>®</sup>  
Lithium-Ion

EcoStruxure<sup>™</sup> Micro  
Data Centre S-Series

apc.com/edge

Life Is On | APC  
by Schneider Electric

## Blackbaud hack leaves UK institutions exposed

Continued from page 1

Questions are also being asked about why Blackbaud took weeks to inform its customers of the hack. Under General Data Protection Regulation (GDPR), companies must report a significant breach to data authorities within 72 hours of learning of an incident or risk potential fines.

A spokesman from the UK's National Cyber Security Centre said: "We are aware of this incident and are supporting partners in the UK and internationally in response. We would urge all organisations to read our guidance on how to defend themselves against malware and ransomware attacks."

The UK's Information Commissioner's Office (ICO) said that 125 organisations had reported to it in relation to the incident "so far" when *Networking+* went to press. ■



**Andrea Babbs, head of sales UK and Ireland at Vipre told *Networking+* that the Blackbaud ransom attack demonstrates the importance of a layered approach to IT security**

## Puppet DevOps adds module support, patching automation

DevOps software provider Puppet has updated its Puppet Enterprise infrastructure automation platform, with capabilities including access to pre-built modules as well as patching task automation.

Version 2019.8 LTS lets customers use thousands of open source and Puppet-built modules in the Puppet Forge catalogue to manage Plans, which enable running a series of tasks through a single command in the Puppet Enterprise console. Users can expand automation to more far-reaching infrastructure use cases, mixing and matching imperative tasks with declarative model-based automation.

Puppet now provides a path from the fast start of the Puppet Bolt orchestration tool and Puppet Forge content to orchestration workflows to provide continuous automation. For example, preparing infrastructure for an application release might include a task set for draining a load balancer, calling VMware to provision an Apache HTTP server, applying patch updates, configuring the database, and related tasks.

"Application deployments are increasingly waiting on DevOps and platform teams to carry out complex sequences of infrastructure configuration, which, when done manually, also increases the risk of errors and disruption," said Abby Kearns, Puppet CTO. "These teams start off making fast progress with basic automation tools, but hit a roadblock once requirements become more complex."

To improve compliance and security,



**Puppet now provides a path from the fast start of the Puppet Bolt orchestration tool and Puppet Forge content to orchestration workflows to provide continuous automation**

the Puppet Enterprise release also includes patching task automation content for Windows and Linux systems, along with an improved user experience in using patching automation in an enterprise. An OS Patching service is available to help

standardize and scale patching processes. The new release also features an upgrade pre-check module that conducts a readiness assessment and finds potential risks and what changes are necessary before conducting an upgrade. ■

## 'UK is the fourth most exposed country for cyber vulnerabilities'

The UK is the fourth most exposed country to cyber vulnerabilities in the world, according to new research.

Rapid7's National Industry Cloud Exposure Report (NICER) for 2020, which placed Britain behind the US, China and South Korea, also found that despite significant efforts on the part of the UK National Cybersecurity Centre (NCSC) to encourage exposure reduction across all organisations, the UK's share of SMB servers has increased by 22% from the same period in 2019.

However, the increase in SMB was offset by a 21% reduction in exposed Telnet services and 11% reduction in exposed FTP services.

Although the UK has fewer total vulnerabilities per-exposed service/system than other countries, due to continued efforts

by the NCSC, these vulnerabilities account for under 38.4% of all exposed surfaces.

The report offers a data-backed analysis of the changing Internet risk landscape, measuring the prevalence and geographic distribution of commonly known exposures in the interconnected technologies that shape our world.

Rapid7's research team calculated a country's risk by measuring the total attack surface, (which reviews how much of a business is exposed to attacks); the total exposure of selected surfaces such as SMB and Telnet (which should never be exposed); the number of CVEs present, as more known vulnerabilities means more exposure; the distribution of vulnerability rates and the maximum vulnerability rate. ■



**Although the UK has fewer total vulnerabilities per-exposed service/system than other countries, due to continued efforts by the NCSC, these vulnerabilities account for under 38.4% of all exposed surfaces**

## 'Universities failing to provide adequate security training'

UK universities are not acting quickly enough to educate about cyber threats, with 46% of staff receiving no training and 12% of universities not offering any kind of security guidance to staff and students.

A recent report from security firm Redscan found that 54% of UK universities reported a data breach to the Information Commissioner's Office in the last year. However, a majority of universities are still found lacking when it comes to imparting cyber security training to staff and students, expenditure on security, carrying out pen testing, or hiring cyber security professionals.

Information obtained by the security firm from 134 universities in the UK via a Freedom of Information request revealed that even though universities are the target of millions of phishing emails every year, the average university is spending just £7,529 per year on security training and is hiring only three qualified cyber security professionals.

Universities often suffer data breaches due to errors committed by employees when storing or handling the personal data of staff and students. Such data leaks or breaches can be avoided if staff are provided adequate cyber security training and

are educated about various online threats.

However, Redscan found that only 66 out of 134 UK universities have Cyber Essentials or Cyber Essential Plus certification, 49% are not proactive in providing security training and information to students, 12% of universities do not offer any kind of security guidance, support or training at all to students, and 46% of all university staff in the UK received no security training in the last year.

"UK universities are among the most well-respected learning and research centres globally, yet our analysis highlights inconsistencies in the approach institutions are taking to protect their staff, students and intellectual property against the latest cyber threats," said Mark Nicholls, CTO of Redscan. "The fact that such a large number of universities don't deliver cyber security training to staff and students, nor commission independent penetration testing, is concerning. These are foundational elements of every security programme and key to helping prevent data breaches."

Nicholls added that "even at this time of intense budgetary pressure", institutions need to ensure that their cyber security teams receive the support they need to defend against "sophisticated adversaries". ■

### EDITORIAL:

**Editor:** Robert Shepherd  
roberts@kadiumpublishing.com

**Designer:** Sean McNamara  
seanm@kadiumpublishing.com

**Contributors:** Gerry Moynihan,  
Pat O'Connor, Tu Jiashun, Rick  
Goud, Justin Godfrey-Cass

### ADVERTISING & PRODUCTION:

**Sales:** Kathy Moynihan  
kathym@kadiumpublishing.com

**Production:** Suzanne Thomas  
suzannet@kadiumpublishing.com

**Publishing director:**  
Kathy Moynihan  
kathym@kadiumpublishing.com

*Networking+* is published monthly by:  
Kadium Ltd, Unit 2, 1 Annett Road,  
Walton-on-Thames, Surrey, KT12 2JR  
Tel: +44 (0) 1932 886 537

The contents of the magazine may not be reproduced in part or whole, or stored in electronic form, without the prior written consent of the publisher. The views expressed in this magazine are not necessarily those shared by the editor or the publisher.  
ISSN: 2052-7373

# UK government announces Huawei U-turn

The UK government has announced a series of measures to remove China's Huawei tech from the UK's 5G mobile networks.

It will ban domestic mobile providers from buying new Huawei 5G equipment after the end of this year and they will have to remove all of its 5G kit from their networks by 2027.

The government had previously said Huawei could be involved in the project but it changed its mind following growing security concerns about China.

However, many in the UK IT arena told Networking+ that the decision was myopic and could have negative consequences.

Gregg Knowles, technology director at plan.com said the decision removes much of the choice previously enjoyed by businesses when it comes to choosing their network provider, and introduces real risk that SMEs must evaluate. "Any CTOs or IT managers who selected Huawei to supply their telecom needs prior to this decision may justifiably feel they have been stung badly," he added. "It may be the case that with this move, firms' evaluation of providers will no longer be based on who is technologically or even commercially the

best supplier, but will be dictated by which supplier they may be able to do business with long term, and which will definitely be able to fulfil their obligations."

Paul German, CEO at data security technology provider Certes Networks, described the move as a waste of time, money and resource – at a time when businesses can ill afford the distraction from core business operations.

"Quite simply, the real issue to be addressed is that network security does not equate to data security; the data always needs to be secure, even when the network isn't and a data assurance solution is all that's needed to combat the problem," he said. "Data assurance requires a strict separation of duties between the security and infrastructure

teams, to ensure infrastructure choices, such as what we see here with Huawei, do not have the potential to adversely affect the required data security posture. On top of this, regulatory compliance is becoming more complex; each iteration widens the scope for required data security controls and often results in point solutions, added complexity and the loss of network visibility further impacting the agility of the organisation to meet the required data assurance posture."

At the heart of the debate is whether the West can trust Huawei or if it will leave its equipment and communication networks and people's mobile phones vulnerable.

However, removing Huawei equipment from the networks will have a significant

impact on the roll-out of the UK's 5G technology. The culture secretary Oliver Dowden said it would be delayed by up to three years and with added costs of circa £2bn.

German added that whether one data classification or multiple, organisations can use crypto-segmentation to micro-segment data flows, protecting against the lateral movement of threats whilst also ensuring all data in motion is secure using policy defined and owned by the security team with keys only they have access to. "With a software-defined approach, security teams can retain control of the data security posture at all times, without compromising network performance or the agility needed to meet on-going goals of the organisation," he said. ■

## Ambulance service makes tracking system enhancements

An ambulance service that receives a 999 call every 40 seconds has enhanced the tracking system of its life-saving kit.

East Midlands Ambulance Service (EMAS) will use the RFID system, upgraded to operate under the Android-based platform, to improve equipment monitoring, maintenance and compliance procedures.

The upgrade was conducted by specialist software firm CoreRFID which installed the original RFID system five years ago, replacing a manual tracking system.

Its RFID solution uses electronic tags attached to each piece of kit which are scanned by special readers. These detect the tags from up to two metres away without needing a line of sight. The information, such as serial numbers, is then automatically downloaded to the EMAS' database, which keeps the team updated on the kits' last location and condition.

"My team needs to be able to find kit and know it's safe for patient use, having passed all compliance tests," said Steve Farnworth, general manager at EMAS. "We manage 650 vehicles across six counties, each carrying several pieces of vital life-saving equipment. The RFID system assists us in monitoring this equipment efficiently and effectively."

Richard Harrison technical sales director at CoreRFID added: "RFID enables emergency service teams to accurately track and improve procedures with less resource needed than manual systems. While RFID is an established solution, emergency services can upgrade their systems to meet new challenges and take advantage of improved software and readers becoming available."

CoreRFID has provided tracking solutions to the NHS, such as Addenbrookes Hospital, as well as Medical Gas Solutions which supplies oxygen and nitronox gas cylinders to NHS trusts, ambulance and fire services. ■

StorageCraft  
**OneXafe Solo**  
 Plug-and-Protect  
 Direct-to-Cloud Backup Appliance

Try-then-Buy Program

**FREE** for 45 Days\*

StorageCraft  
 OneXafe Solo

**TECHNOLOGY  
 2020 RESELLER  
 EDITOR'S CHOICE AWARD**  
 STORAGECRAFT: OneXafe Solo

## Feel the heat: putting liquid cooling front and centre in the data centre



Higher density chips are on the way. Liquid-cooled IT equipment is not new. It's been around for decades but recently has gained interest for more mainstream data centre applications. We tend to hear about it for niche solutions – such as for high-performance computing (HPC) and gaming. But today, there are some key trends and drivers that make it an appealing solution for the more mainstream IT audience. While **data centre and edge environments** today are primarily air-cooled, we are seeing a growing interest and value in the adoption of liquid cooling. The applications of cloud, IoT, AI, and edge are driving the continuous increase of chip and rack power density. There's also a continued focus on energy efficiency and cost. For many applications, liquid cooling is the optimal cooling solution. Today, air and liquid cooling options exist but many work harder, not smarter. Enter chassis-based immersive liquid cooling to solve the server chaos with the potential to optimise operations, efficiency, and cost.

Compared with conventional air cooling, liquid cooling provides benefits for data centre owners such as higher energy efficiency, smaller footprint, lower TCO, enhanced server reliability, lower noise, etc. However, liquid cooling also has some drawbacks such as higher investment, retrofit or redesign of servers, new data centre operation and maintenance skills required, etc

**Join our webinar** and find out how data centre owners can make an informed decision on whether liquid cooling has advantages for their application. This webinar session will focus on the major liquid cooling methodologies, the tradeoffs they bring in different environments and how Schneider Electric is leading an eco-system to create viable, commercial liquid-cooled systems that offer up to 15% lower CapEx and up to 30% energy reduction.

**Register to attend.**

## Aryaka partners with Check Point Software

Aryaka has forged a partnership with Check Point Software Technologies that leverages the former's Cloud-First managed SD-WAN solution, Check Point CloudGuard Connect and CloudGuard Edge to deliver integrated security and SD-WAN as-a-Service. Check Point CloudGuard technology delivers threat

prevention that is updated in real-time using the latest Check Point ThreatCloud intelligence. The partnership delivers customers a unified threat and access management platform that has the flexibility to deploy branch office security in minutes, while reducing operational expenses by up to 40%.

## New 'Work IN' Service for SMEs

Technology as a service specialist IntraLAN, has launched Work IN, a new IT and connectivity service built for SMEs with home-based, remote or distributed workforces. Described as "affordable an easy to manage", the service is said to ensure the user receives the same robust IT service as they would in the corporate office. The company also said the employer knows that IT and data protection policies are being adhered to. Available in three tiers and starting from £40 per month, every package includes a business grade managed firewall and Wi-Fi router with plug-and-play portability, power-over-ethernet, remote monitoring and support, next working day replacements, and full user on-boarding.

## Sale signs Acronis to boost defence

Premiership rugby club Sale Sharks has named Acronis as its official cyber protection partner. Under the terms of the agreement, Acronis will provide the club with access to state-of-the-art cyber protection solutions for critical data assets. In addition, Acronis will also help analyse collected data with the help of AI and machine learning (AI/ML) technology to enhance on-pitch performance. Sale Sharks are the first professional rugby team to sign Acronis as a cyber protection partner. Acronis has formed multiple sports partnerships with professional teams in football, American football, formula one, baseball and more.

## Finance teams targeted as email attacks rise by 22%

Two out of three UK companies (66%) suffered brute force attacks against Microsoft 365 accounts during the past three months – up from 48% in the first quarter. A report conducted by bluedog Security Monitoring found that around 8% of all companies suffered breaches in the second quarter as a result of the attacks. The company has also seen a 22% rise in phishing attacks targeting the creation of apps within Azure. It believes every company is now being targeted at least once a week by this type of attack and in some cases, five or six times a day.



## MCC agents operate from anywhere with move to cloud

Manchester City Council (MCC) has selected integrated cloud communications platform provider 8x8 to keep vital services running safely for its more than half a million residents throughout lockdown. Supporting one of the largest metropolitan districts in the UK, MCC commenced

a detailed procurement process two years ago, to implement a new cloud-based communications solution in line with its wider cloud-based ICT strategy. Nearing the end of the process, the 8x8 Open Communications Platform had been selected due to its enhanced flexibility and ability to connect

contact centre agents across voice, video and chat. However, in light of the Covid-19 outbreak and the UK Government's mandate to work from home, the council fast-tracked solution deployment in order to keep vital services running while ensuring the safety for both residents and staff.

## Secure I.T. Environments completes data centre project at Hammersmith Hospital

Secure I.T. Environments, a specialist in the designing and building of modular, containerised and micro data centres, has completed a new data centre project at Hammersmith Hospital, part of the Imperial College Healthcare Trust, which has over 12,000 staff, caring for around 1.5 million patients a year. The Bedfordshire-based firm and the west London hospital decided that the best location for the data centre should be on a ground floor location that offered access and connectivity for the services needed. "Running any NHS data centre project presents a number of challenges, especially when a site is operating 24/7/365," said Chris Wellfair, projects director at Secure I.T. Environments. "We have many years' experience working with NHS Trusts in the UK,



successfully delivering projects on sites where the public and staff are constantly present, and downtime is not an option." He added that "those same skills" help the company to deliver on a number of projects for other sectors including retail, education, manufacturing and telecommunications. Last year, the vendor announced the handover of a data centre project to Thurrock County Council in Essex.

## Covid-19 test to bring back UK sport

A Manchester-based cyber technology firm has put forward pilot programmes to the Department of Culture Media & Sport (DCMS) to help get football, rugby and sports fans back into stadiums following prime minister Boris Johnson's announcement to get stadiums open by October. The pilot programmes called 'Fans Are Back' – widely regarded as 'game changing' in getting sports fans back into stadiums – has also recently been given the support of former sports minister Richard Caborn. VST Enterprises (VSTE) along with its sports partners Redstrike, public safety and event management partners Halo Solutions and occupational health care company Latus Health have put forward the active pilot proposals.

## Cloud and connectivity top IT spending charts

UK enterprises said they are largely spending their IT budgets on tools and services to further enable remote working during the Covid-19 pandemic. According to the latest research from market intelligence service Delta, Cloud IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) and connectivity, including WAN (Wide Area Networks) and networking technologies, top spending plans. Some 16% of respondents expressed an intention to purchase IaaS and PaaS technologies, with 10% said that networking technologies were their priority.

## Word on the web...

**Google is rolling out plans to move Britain's data to the US - but what does this mean for UK firms? Neil Thacker from Netskope reveals all...**

**To read this and other opinions from industry luminaries, visit [www.networkingplus.co.uk](http://www.networkingplus.co.uk)**



# ALWAYS CONNECTED COMMUNICATIONS

*with the Smart Wireless Network*

**Why choose Rajant  
Kinetic Mesh®** to  
transform virtually any  
asset into network  
infrastructure?

**It's ubiquitous,  
connecting people to  
people, people to things  
and things to things—  
mobile, fixed, or both**



**It's resilient  
and self-optimizes**  
as assets are added or  
moved, creating a fully  
redundant network



**It's smart and  
delivers intelligence**  
in real-time with low  
latency, high-bandwidth  
performance



**RAJANT**

**IF IT'S MOVING, IT'S RAJANT.**

Learn how Rajant Kinetic Mesh® can bring IoT to life.  
Request a **free demo** at [rajant.com/np-demo](http://rajant.com/np-demo)

# Why police are turning to cellular

## Justin Godfrey-Cass from Wireless Logic weighs up cellular connectivity over - or in addition to - fixed line infrastructure

Police forces rely on Automatic Number Plate Recognition (ANPR) to help in criminal investigations and traffic enforcement. The technology is used for time-critical issues including detection and disruption of criminality, security, as well as quick and resilient connection and so is paramount to relay information about the location of vehicles of interest back to the police force.

While fixed line infrastructure is usually the default method of connectivity for ANPR, more and more police forces are beginning to turn to cellular connectivity, either to replace a fixed line or as a back-up. Cost, network flexibility and security all come together to create a more suitable solution for tracking vehicles of interest.

Cellular connectivity does make usage more expensive, but the infrastructure and maintenance cost can be significantly more expensive with fixed lines and over a long term period, the total cost of ownership can be notably higher.

Fixed line infrastructure is also logistically difficult to deliver. Because of the locations of some ANPR cameras, fixed line connectivity is not always easily available, and many forces operate deployable ANPR for short term periods, such as events. In instances such as these, where ANPR needs to be deployed quickly and removed a short while later, a fixed line simply wouldn't make sense.

However, even when it is accessible, initial deployment can be very time consuming - sometimes taking weeks or even months to dig up roads in order to lay cables. Further to this, any repairs that may be needed further along the line might also require more digging into roads in order to fix any problems.

Cellular connectivity, on the other hand, can be deployed in a matter of days for a fraction of the cost. Any extra devices, repairs or hardware updates require no new cabling. It also gives police forces the ability to use mobile ANPR - in-vehicle - which would otherwise be unavailable with a fixed line connection.

Where Highways England ensures that motorway networks are fibre connected by default, A-roads and anything smaller have no fixed line access. Cellular connectivity has seamless installation and configuration.

The flexibility offered by cellular connectivity is another big advantage when it comes to ANPR systems, and access to fast and reliable data transfer on a rapid deployment basis is paramount for police forces, who need to be operating at maximum operational efficiency wherever possible.

ANPR cameras allow police officers to track crimes - has a crime taken place in a specific area? Has the camera picked up vehicles associated with

known criminals? Or has it simply caught a suspect vehicle moving away from the scene? The speed of data transmission needs to be immediate and reliable at all times. As such, the networks on which they operate need to offer that speed and reliability.

Through cellular connectivity, that platform is in place. Cameras can be set up with primary and backup networks, to fill in any gaps in signal strength or coverage, all of which can be managed through a single platform.

Furthermore, where fixed lines present a single point of failure, a cellular connection can allow devices access to multiple networks, so different locations can utilise different networks, and can operate through whichever offers the best signal strength. Typically, these cameras use 4G due to bandwidth requirements of the application. However, despite the use of different networks and varying bandwidth needs, everything can be managed simply, without complications, through one platform. This flexibility gives ANPR systems and police force ANPR managers the best opportunity to operate at maximum efficiency, reliably remaining in action ready to be called upon. All networks also can be managed through a single interface, keeping things simple to manage at all times.

Security is another critical factor for ANPR technology. Any IoT application needs security measures in place to protect against any unauthorised access. With ANPR, each camera records and transmits data about every vehicle that passes it, including those vehicles that are not known to be of interest at the time. This, along with the high level of responsibility that police forces have when it comes to handling public data, means that the secure transmission of data is a top priority for ANPR.

Cellular IoT devices - in this instance, ANPR - are able to leverage private network technology, such as certified VPNs and direct physical interconnects in data centres, to help layer security for devices, networks and all data encompassed within. With security being of absolute importance, finding the right partners and solutions is critical. Using providers that follow the guidance issued by the National Cyber Security Center (NCSC) is always best practice, but typically, partnering with an organisation that holds an ISO27001 certification will go a long way to ensuring the security of an ANPR system.

We've started to see more police forces transition towards cellular connectivity in order to lower costs, improve connectivity and keep data secure. Within public sector agendas, security, cost management and resilience are all top priorities. Through cellular connectivity, authorities can easily implement fit-for-purpose camera connectivity solutions, all deployed across a single, safe, cost-effective platform, and it should certainly at least be a consideration for police forces looking to improve their ANPR systems.

Justin Godfrey-Cass, transport solutions business development manager, Wireless Logic

# ACIS™

## More than just a BMS

### HVAC OPTIMISER

Using extensive cooling knowledge and experience to help optimise and manage your data centre HVAC systems.



### BMS

An extensive range of control solutions that deliver intelligent component optimisation for existing plant equipment and systems.



### POWER MANAGEMENT

Powerful monitoring and optimisation solutions for high-power electrical systems keep your system running smoothly.



## ANTENNA SOLUTIONS

### WORLDWIDE ANTENNA SOLUTIONS COVERING 30 MHz to 6 GHz

Superior Antenna Solutions  
 Custom Design Services  
 Knowledgeable Partnership  
 Dependable Customer Service

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

**MobileMark**  
ANTENNA SOLUTIONS

Contact Us Now  
 +44 1543 459555  
[enquiries@MobileMarkEurope.co.uk](mailto:enquiries@MobileMarkEurope.co.uk)

# New Reality: What businesses can learn from the military

Pat O'Connor, managing director & co-founder, VRAI

**W**ith the world exploring new ways to safely work and train, what of those who work and train in high-risk environments as standard? The key to this new normal is VR training, writes Pat O'Connor, managing director of VRAI.

For those of us working from home in the midst of the coronavirus pandemic – most of us – the videoconferencing provider Zoom has certainly become a household name. Not only has the global work-from-home experiment prompted by Covid-19 highlighted the benefits of these remote working tools, it has also illustrated the sophisticated technology that was available to us all along.

As a result, Zoom will be hailed as a company that prospered during the crisis and looking back on previous economic crashes and there is a commonality between the companies that swam and those that sank.

As we progress into financial uncertainty caused by Covid-19, many businesses will become far more conservative in order to survive. Cutting costs, scaling back and bunkering up seems the safest approach going forward. However, if we compare this period in 2020 to the economic crash of 2008, you will see that the most successful companies were those that chose to adapt and embrace change, rather than let the situation or course of events decide their fate for them. Businesses such as WhatsApp, Uber, Airbnb, Instagram and Dropbox were all founded during this time and then went on to become global powerhouses. They still thriving today during the most uncertain of times.

On the face of it there isn't a lot that they have in common, other than being broadly digital companies. For me, the common thread between them is their ability to adapt through the last recession. They spotted a trend of consumerism of people knowing what they want and when they wanted it. With adaptability rather than reclusion at the forefront of their business model, they were able to become some of the most successful companies in the world.

So, what kind of consumer trends are likely to arise as a result of the Covid-19 crisis?

Since countries around the world went into lockdown to slow the spread of Covid-19, the shift towards remote working tools has been rapid. Once the crisis abates, that expansion of the digital workplace is likely to continue. Prior to today, planning for remote work was a low priority for many businesses, largely side-lined as a perk sought for the millennial workforce. In the post-Covid-19 landscape however, businesses who do not adequately prepare their company to work remotely will be considered reckless and may not survive the approaching economic challenges we face.

Video conferencing has allowed business to continue functioning and people to continue interacting, but it has its limitations – especially for those who operate in risky or remote environments. For front line medical staff, offshore technicians and even numerous manufacturing settings, there is a need to train for, prepare for and mitigate risk.

After all, traditional e-learning tools cannot prepare someone to climb a high voltage electricity pylon in a storm, or fix a blade on a 110m high wind turbine 100km off the north coast of Scotland.

Where can business leaders look to for guidance on how to prepare their employees

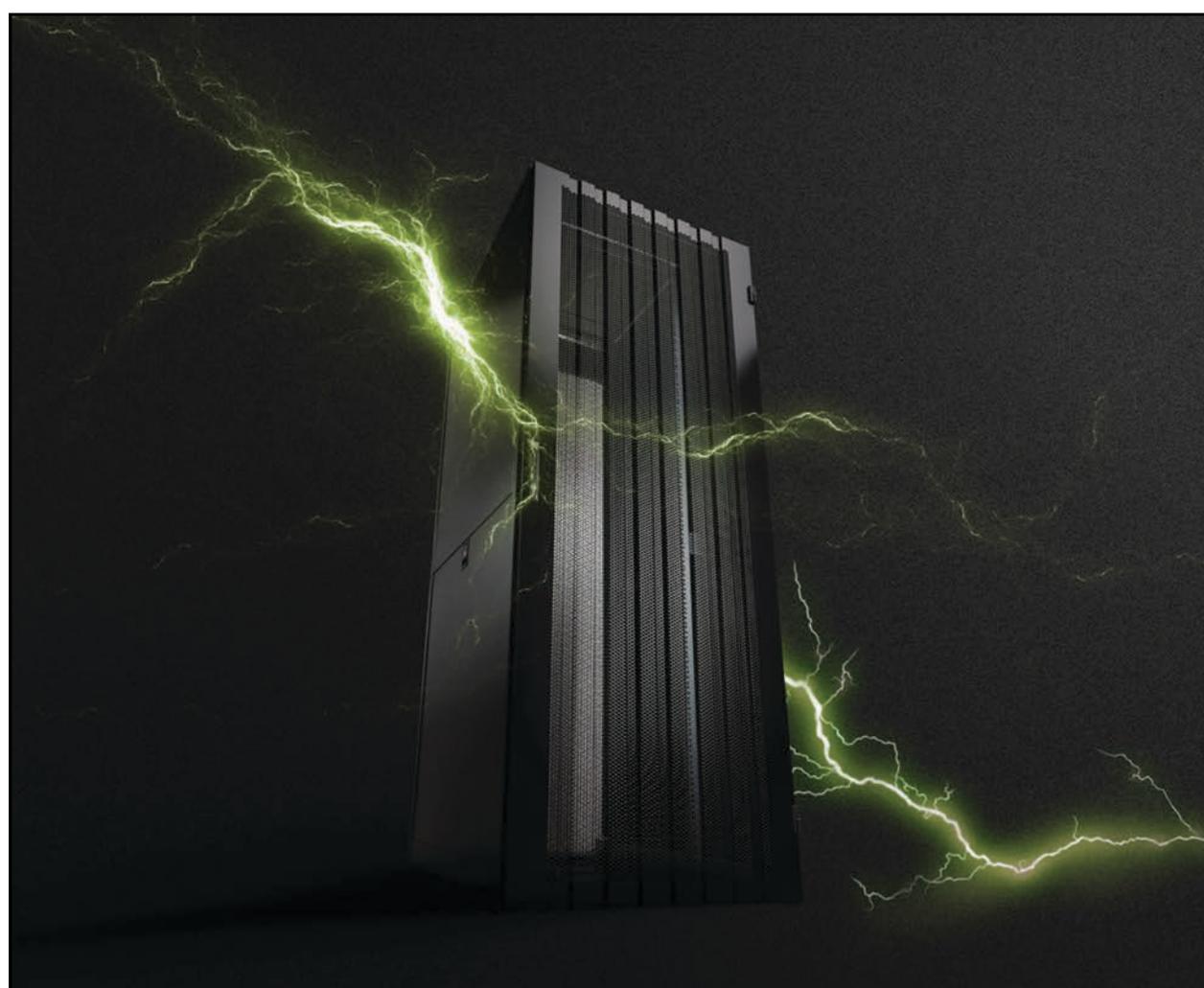
in this unpredictable world? I believe the answer lies in the military. That's because the military has been using simulation training for decades as a way to replicate risky, remote and difficult to replicate scenarios that soldiers are likely to encounter at some point. Sometimes the simulation was in order to avoid the prying eyes of adversaries, sometimes simulation was about cost saving and sometimes it was simply about utility – simulation training was better and easier to do than traditional training.

However, until recently, military

simulation training was often reserved for high value roles like fighter pilots, or ships captains, who trained in "sim centres". These sim centres had traditional simulators with complicated hydraulics and expensive replicas of the real world equipment. There is now a paradigm shift occurring in military training towards providing virtual simulation at the point of need. The training is contained in a VR headset that a soldier can use while in a hangar waiting for rotation flight, or a winchman can use during a "weather day",

or a ships engineer can use while hundreds of kilometres away from the naval college.

The added value of VR simulation is that its inherent data capture capability can be used to provide deep insights into how individuals learn and perform. Furthermore, the addition of physiological sensors can allow you to know not just what people do, but also how they feel when they do it. These data driven insights can transform our ability to reduce risk for our employees and ensure they are confident in performing the tasks that they will face in reality.

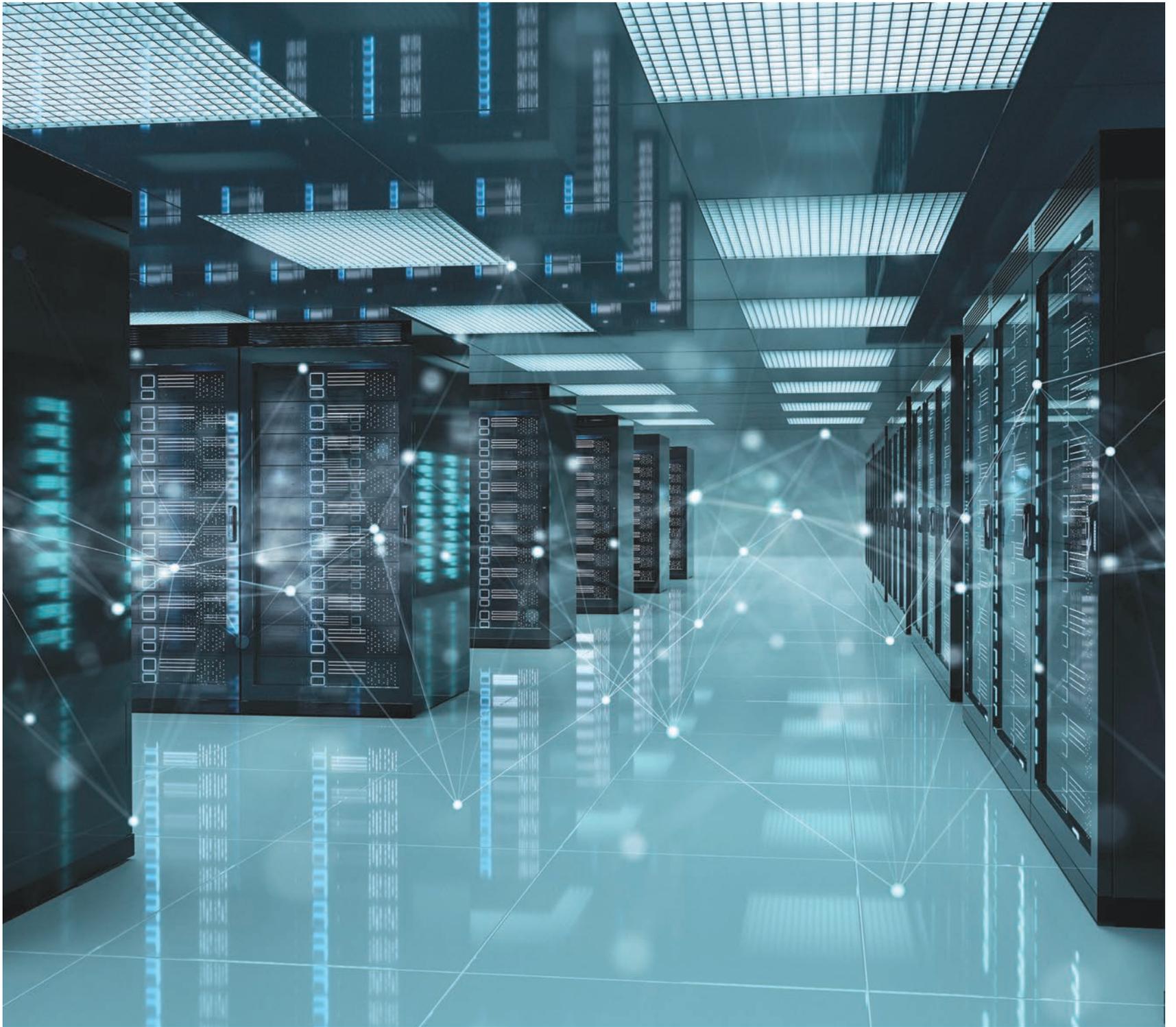


## BIG ON PERFORMANCE

When compromised performance is not an option our rack solutions deliver style, flexibility and specification options each and every time. With integral cable management, doors to encourage maximum ventilation, up to 1300kg load bearing, free next day UK delivery and 25 year warranty, you can be sure you are getting the best in performance when you choose an Environ rack from Excel.

Visit Environ:  
[excel-networking.com/environ-racks](https://www.excel-networking.com/environ-racks)

**excel**  
without compromise.



# AI in data centres

**AI is a cool futuristic term we have been using for a number of years. Now, in 2020, it's time to find out what it actually does for data centres. Robert Shepherd speaks to the geeks**

**A**dmit it, the first time some of you heard of 'Artificial Intelligence' was following the release of A.I. - the eponymous 2001 motion picture, developed by Stanley Kubrick in the 70s and directed by Steven Spielberg decades later.

It was to be the former's first foray into the science-fiction genre since his 1968 sci-fi classic 2001: A Space Odyssey, a prescient allegory about how destructive artificial intelligence can be when cruelly misused. The point is visionaries like the Hollywood creatives foresaw how useful it could be to humankind before most people reading this were born.

Now, fast-forward to Gartner's 2019 CIO Survey, which highlights the fact that number of enterprises implementing AI tripled in the past year. However, Gartner

also claims that more than 30% of data centres that don't deploy AI and machine learning won't be operationally and economically feasible by 2020.

Still, before even understanding the potential use cases for data centres, John Yardley, CEO, Threads Software, says it's prudent to first understand what AI means. "It was, of course, Alan Turing who originally coined the term machine (or artificial) intelligence to define the machine behaviour that is indistinguishable from that of human," he adds. "So, when you ask Siri lots of questions and it gives you the answers you would expect, you might regard that as artificial intelligence. In fact, Siri may be simply doing a web search which is just looking up millions of web resources. To the user, that is just as intelligent as an application that is

modelling the human brain. In fact, it is the speech recognition that is the AI rather than web search, but the user would not necessarily perceive it that way." Yardley says that "it is also important to realise that the human brain is a computer" and that "there is technically no reason" why its behaviour could not be modelled in silicon - together with all the emotions we perceive as "human".

Robots can carry out the vast majority of functions we mere mortals have always carried out ourselves and Yardley sees a lot of benefit in that.

"Computers do not get tired, want pay rises, get sick, or throw tantrums," he continues. "AI is simply another form of automation, just like the Jacquard machine (a device fitted to a loom that simplifies the process of manufacturing textiles with complex

patterns) was. It displaces humans, but the replaced humans can then be deployed to do things computers cannot yet do. Humans are not good at repetitive boring tasks."

Yardley adds that in the data centre, there are many such tasks. "Filing responses, looking up records, pre-empting questions and so on," he continues. "What AI can do is find connections that humans cannot, or at least, much more quickly, such as establishing that certain sorts of customer have certain sorts of questions. Huge amounts of information is conveyed in people's voices that might not be recognised by a human, but detectable by a computer."

For Peter Ruffley, chairman at data specialist Zizo, "the IT industry is doing itself no favours" by promising the earth with emerging technologies, without having

the ability to fully deliver them. “See Hadoop’s story with big data as an example and look where that is now,” he says. “There is also a growing need to dispel some of the myths surrounding the capabilities of AI and data-led applications, which often sit within the c-suite, that investment will give them the equivalent of the ship’s computer from Star Trek, or the answer to the question ‘how can I grow the business?’ As part of any AI strategy, it’s imperative that businesses, from the board down, have a true understanding of the use cases of AI and where the value lies.” Ruffley adds that if there is a clear business need and an outcome in mind then AI can be the right tool. “But it won’t do everything for you,” he warns. “The bulk of the work still has to be done somewhere, either in the machine learning or data preparation phase.”

Understanding how something works is clearly the most important thing, but then you have to understand “what the whole strategic vision is and look at where value can be delivered and how a return on investment (ROI) is achieved”. That’s Ruffley’s view and he says what needs to happen is for data centre providers to work towards educating customers on what can be done to get quick wins.

“Additionally, sustainability is riding high on the business agenda and this is something providers need to take into consideration,” he adds. “How can the infrastructure needed for emerging technologies work better? Perhaps it’s with sharing data between the industry and working together to analyse it. In these cases, maybe the whole is greater than the sum of its parts. The hard bit is going to be convincing people to relinquish control of their data. Can the industry move the conversation on from being purely technical and around how much power and kilowatts are being used to how is this helping our social corporate responsibility/our green credentials?”

Ruffley also highlights a number of innovations already happening, where lessons can be learnt. In the Nordics, for example, there are those who are building carbon neutral data centres, which are completely air cooled, with the use of sustainable power cooling through solar. “The cooling also comes through the building by basically opening the windows,” he adds. “There are also water cool data centres out there under the ocean.”

Jonathan Martinez, commercial control systems manager at data centre cooling solutions provider Airedale says there are a number of benefits arising from the use of AI/machine learning within a data centre environment, which Airedale is developing within the ACIS AI framework. “One of the big ones being the ability to autonomously



**Looking to the future, will real life resemble a Hollywood sci-fi movie in that everything will be run by AI, or will we always need humans on standby?**

optimise the HVAC system to ensure it is always running at peak efficiency,” he says. “Often cooling systems are ‘set and forget’ once commissioned, however variables such as data centre IT load and outside ambient temperature can vary throughout the course of the year. The cooling system in its commissioned state is sized to deal with these fluctuations, however at peak load may not be operating at peak efficiency.”

Martinez says a machine learning algorithm can learn the patterns associated with these variables and determine over time what changes it can make to optimise the efficiency of the plant during the pattern cycle. “If the system can predict when these peaks will happen, then it can take action prior to these peaks to ensure the system is best armed to deal with the spike in the most efficient way,” he adds. “This could be adjusting chilled water setpoint, altering airflow, or reducing pump setpoints for example. In short, an AI system in theory could make constant minute adjustments to the system throughout the year to improve efficiency based on pattern recognition, far better than a human could.”

Then, of course, there’s that old debate of AI ready vs. AI reality and Ruffley questions why with IoT, many organisations are chasing the mythical concept of ‘let’s have every device under management’. He continues: “But why? What’s

the real benefit of doing that? All they are doing is creating an overwhelming amount of low value data. They are expecting data warehouses to store a massive amount of data. If a business keeps data from a device that shows it pinged every 30 seconds rather than a minute, then that’s just keeping data for the sake of it. There’s no strategy there. The ‘everyone store everything’ mentality needs to change.”

Indeed, he says one of the main barriers to implementing AI is the challenges in the availability and preparing of data. He claims a business cannot become data-driven, if it doesn’t understand the information it has and the concept of ‘garbage in, garbage out’ is especially true when it comes to the data used for AI.

Ruffley predicts that over the coming years, the world will see “a tremendous investment in large scale and high-performance computing (HPC) being installed within organisations to support data analytics and AI.

“At the same time, there will be an onus on data centre providers to be able to provide these systems without necessarily understanding the infrastructure that’s required to deliver them or the software or business output needed to get value from them,” he says. “We saw this in the realm of big data, when everyone tried to swing together some kind of big data solution and it was very easy to just say we’ll use Hadoop to build this giant system. If we’re not careful, the same could happen with AI. There’s been a lot of conversations about the fact that if we were to peel back the layers of many AI solutions, we’ll find that there is still a lot of people investing a lot of hard work into them, so when it comes to automating processes, we aren’t quite in that space yet. AI solutions are currently very resource heavy.”

He says “there’s no denying that the majority of data centres” are now being asked how they provide AI solutions and how they can assist organisations on their AI journey. “Whilst organisations might assume that data centres will have everything to do with AI tied up. Is this really the case?” Ruffley continues. “Yes, there is a realisation of the benefits of AI, but actually how it is best

implemented, and by who, to get the right results, hasn’t been fully decided.”

If you know anything about AI, then you’ll have heard of the ‘black box problem’, because like the human brain, it is hard to understand from the outside. The black box is used for decision-making, often based on machine learning over big data, mapping a user’s features into a class predicting the behavioural traits of individuals, without exposing the reasons why. As you can imagine, it can be problematic not only for its lack of transparency, but also for possible biases inherited by the algorithms from human prejudices and collection artifacts hidden in the training data. That’s because they can lead to unfair, unexpected or wrong decisions.

Ted Kwartler, VP, Trusted AI at enterprise AI specialist DataRobot, says AI in the datacentre faces the same challenges as AI in any other industry or application. “When the ‘black box problem’ in AI is raised, in response, some may focus on the evolving techniques that allow us to probe, stress-test, or challenge the opaqueness of our models,” he says. “Others may point to the fact that ‘explainability’ should inform model selection. Depending on the use case, some modelling techniques support transparency far better than others without sacrificing performance. There’s no such thing in machine learning as one-size-fits-all.”

However, Kwartler warns of “a bigger and actually even more vital question lurking underneath the ‘black box problem’.” He says: “Why is it so important to explain a model’s decision? If a model performs perfectly – if its decision-making is flawless – we wouldn’t worry so much about explaining how it works, besides learning from it. However, no such model exists in real life. So, when we’re talking about an algorithm making a decision of high-impact on a person’s well-being, for example, and maybe getting it wrong, we need to be able to do more than just explain a bad prediction. We want to be able to prevent it.”

Perceived wisdom would dictate that the underlying issue is how to establish trust in a model’s decisions. That’s

**“As part of any AI strategy, it’s imperative that businesses, from the board down, have a true understanding of the use cases of AI and where the value lies.”**

*Peter Ruffley,  
chairman,  
Zizo*



because AI models from development to production need operational guardrails to ensure trustworthy behaviour, adds Kwartler. "In model training, building trust first means interrogating the data: its integrity, diversity, appropriateness and quality," he continues. "Model selection is then often a negotiation of trade-offs, balancing accuracy, speed and explainability across a variety of suitable techniques. And finally, in production, proper governance requires humility: the ability to recognise how confident a prediction is and if there are quantifiable reasons to be unsure of it. If so, a human-in- or human-over-the-loop should be empowered to intervene and guarantee that a safe decision is made. Explainability is possible in AI, but achieving it is not the finish-line for actually building a model you can trust."

Yardley again invokes World War II when he explains that the German Enigma machine – Turing as we know cracked its codes – was a good example of a black box in that it is unlikely any of the operators knew or cared how it worked. "In contrast, the data encryption standard (DES) is not a black box - the way it works is public," he adds. The strength of the DES is in the algorithm itself, not in it being secret."

So, is the 'black box problem' a serious one? Yardley certainly thinks so. "Not because we need to know how AI works but because a black box approach discourages developers from understanding the problem they are solving," he says. "Take neural network approaches to speech recognition. These work well at recognising speech but the developers have no idea why they work - that is, the developers know nothing about acoustics, semantics, linguistics, and so on, and nor do they need to know. They tend to assume that the more computing power is applied, the better the result. However, relying solely on historic examples to predict future performance usually results in hitting a dead end and having no idea what to do."

"With any system that we don't fully understand, we cannot predict its behaviour," he continues. That could have legal and even potentially more serious implications."

Martinez agrees that the black box issue is a valid concern. "Techniques such as linear regression, by design, are more interpretable compared to techniques such as deep learning," he says.

"However, interpreting deep learning models aka 'explainable AI' is a hot topic of research and there are multiple ways to mitigate the issue. There are multiple machine learning toolboxes to extract additional information from machine learning (ML) models in general, Google have a decent suite of these already. One of the design requirements of the AI solutions we are developing at Airedale, is for the system to be fully interpretable in order to avoid the 'black box problem.'"

Looking ahead to the future, will real life resemble a Hollywood sci-fi movie in that everything will be run by AI, or will we always need human hands on standby?

Nevertheless, Ruffley warns, that lots of data centres "jumped in headfirst" with the explosion of big data and didn't come out with any tangible results. "If we're not careful, AI could just become another IT bubble," he says.

Nevertheless, Ruffley says "there is still time to turn things around", because as we move into a world of ever-increasing data volumes, we are constantly searching for the value hidden within low value data that is being produced by IoT, smartphone apps and at the edge.

"As the global costs of energy rise, and the numbers of HPC clusters powering AI to drive our next generation technologies increase, new technologies have to be found that lower the cost of running the data centre, beyond standard air cooling," he continues. "It's great to see people thinking outside of the box on this with, with submerged HPC systems and full, naturally aerated data centres, but more will have to be done (and fast) to meet up with global data growth. The appetite for AI is undoubtedly there but for it to be able to be deployed at scale and for enterprises to see real value, ROI and new business opportunities from it, data centres need to move the conversation on, work together and individually utilise AI in the best way possible or risk losing out to the competition."

As far as Yardley is concerned, "If

**"Others may point to the fact that 'explainability' should inform model selection."**

Ted Kwartler, vice president, DataRobot

we can clone a human brain, it will act indistinguishably from the human's brain it was cloned from". He says: "That may take another 100 years, but if we don't self-destruct, it will happen. That of course raises many questions about the future of the human race."

That's a much deeper discussion for another time and place. It's also a good stimulus for another Hollywood blockbuster. ■



**EnGenius**

Visualize Your Network with  
**AI-Driven EnGenius Cloud**

[www.engeniusnetworks.eu](http://www.engeniusnetworks.eu)

Supported Devices of EnGenius Cloud

# A winning streak

## Three rugby clubs gets tech upgrades for a winning future



### Kendal RUFC's state-of-the-art upgrade

Kendal RUFC's move away from its home for nearly a century was always going to attract considerable interest and great expectations from the local communities, given the investment in a dedicated new state-of-the-art £8m stadium.

The new Mintbridge Stadium sits just a stone's throw from the old ground, but the new facilities are light years ahead of the Club's historic home. The old ground was historically referred to by Kendal's supporters as a 'northern fortress' and modern incarnation is certainly an imposing and impressive site.

Along with the expected facilities for playing teams, Mintbridge is also a function venue with its own commercial restaurant kitchen and bars servicing the lounge bar and Kentdale Suite with a capacity for around 200 guests. For players and public, there is a new gymnasium with personal training and physiotherapy also available.

A modern, busy and versatile stadium that caters for both the sporting and business ambitions of the Club and community, yet one with diverse and dedicated IT solutions.

Adam Blamire is the lead engineer at iTek Computer Solutions and, as well as being a supporter of KRUFRC, was instrumental in much of the design, installation and support of the IT systems at Mintbridge Stadium.

"This was in the very earliest stages of the project, so we weren't exactly providing costs for defined requirements, we were designing an entire stadium's IT infrastructure from the ground up."

iTek's proposal was accepted, but it wasn't until the stadium was nearing completion that they were called upon to install and commission their system.

"It was quite a different project for us as we didn't inherit anything, it really was a blank canvas. Although we had been able to advise, inform and provide our input on what was needed during the planning stages it was pretty much the eleventh hour when we got on-site."

"That said, being involved at an early stage meant that when we were scheduled to undertake the installation everyone knew the plan and it was a relatively quick project to complete, given the size of the site."

The specification for the stadium was one which evolved from conversations with the Mintbridge team, with requirements understood and plenty of foresight provided by iTek to help ensure any system could be as future proof as possible and allow for integration with a diverse array of external hardware and software.

The list of equipment and services provided by iTek is extensive and includes

new PCs, servers and networking throughout the site with robust security systems and firewall protection. The many email accounts required by such a large operation are also hosted by iTek, again, with high levels of cyber security.

"Security is paramount, especially with multiple businesses and operations on-site so we built their server so that different people have access to specific areas, with appropriate permissions and passwords etc."

It is anticipated that on bigger match days there will be around 2,000 supporters at the ground, all potentially wanting to access the stadium's Wi-Fi.

"We set-up Wi-Fi for both corporate and guests – on match day, or events and weddings, the internet will take some real hammer, so we proposed a dedicated line as a solution. We worked in consultancy with the team at Mintbridge to specify what was required and helped negotiate with Zen Internet on the installation of the service. What's now in place delivers speeds of 100Mb both up and down and offers 100% up-time."

The firewall put into place around this and IT perimeter security (inbound and outbound) means that staff and supporters can enjoy quick and safe access to the web, wherever they are on the site.

"The Wi-Fi coverage is impressive and can be accessed from anywhere on site, including the far side of the all-weather training pitches over 100 metres away from the main stadium."

Staff training was also provided as part of the hand-over, the 'user acceptance' stage confirming that everyone was happy with the new IT in all its different guises.

With so many different third-party systems and hardware on the site, it was critical that iTek's network could 'talk' to everything, from the pitch-side electronic scoreboard to the front gate ticketing system and everything in-between.

Even the stadium's VOIP phone system has been provided by iTek. "It's not something we'd consider a core service, but we have supplied and installed for a number of businesses; I have to say it's something we do very well. Of course, a decent broadband connection and good networking is key, but get the right system and it becomes a very cost-effective solution for any business," adds Ben Mitchinson, MD at iTek Computer Solutions.

"Our ongoing service for Mintbridge Stadium invariably means we help support other supplier's hardware; it may not be something that we have supplied but if there is an issue then we are happy to get involved and work to provide a fix," continues Ben, "We can test if our systems are working fine and help identify any issue beyond there, it's all part of the service."



### Munster gets smart

Over-C, a provider of workplace management and analytics which uses location, sensor data and other IoT devices to empower frontline workers, worked with Thomond Park Stadium, the home of Munster Rugby Club to transform it into a smart stadium.

The bespoke digital solution will help Thomond Park to streamline processes, gain new insights into stadium data and deliver a first-rate fan experience.

Thomond Park Stadium was using paper-based processes for up to 1,500 contractors to perform hundreds of match day security, catering, cleaning and maintenance tasks. These critical tasks included checking all fire exits, fridges, boiler rooms, public facilities, fire safety equipment, waste disposal, collaboration with local authorities and transport as well as many more.

The day-to-day management team were finding it extremely problematic and time consuming to gather all of the required data, report on it and identify trends, performance and risk. They were also struggling to communicate and collaborate effectively with all staff and contractors. They needed to spend more time on delivering a great fan experience instead of administrative, manual, time-consuming tasks.

"We were running on a very manual system previously," says Colm Moran, operations facility and event manager, Thomond Park Stadium. "Now every last detail which occurs in the stadium can be put onto the Over-C system, which is so vast that I can't actually see the end to its capabilities. We are planning to use the Over-C system further to ensure our fan experience is second to none – from our toilets, to our gates access to ensure the highest customer standard is delivered."

Mike Elliot, CEO and founder adds, "After sitting down with the Thomond Park team we immediately began to understand their specific requirements and worked with them to create a Smart Stadium solution. Our solutions help automate and digitise their processes giving them better visibility and full transparency into their operations all from one platform."

Through strategically placed wireless sensors and other IoT endpoints throughout the stadium, data is captured based on the information they want to collect whether it's temperature, humidity, motion or other. These sensors also trigger different tasks and workflows with all data available in real-time through a visual dashboard.

Moran continued "We can historically go back over the data and see where the trends are happening and analyse that data to make decisions going forward."

Over-C's system enables Thomond Park to meet these government guidelines while achieving and maintaining ISO 20121, without compromising fan experience or overpaying for services.



### Ulster Rugby's new Wi-Fi service

Ulster Rugby is one of four professional teams in Ireland who compete in the Guinness PRO12 Championship and the European Rugby Champions Cup. Kingspan stadium has an overall capacity of 18,200, with four fully covered terraced areas providing seating for up to 9,000 spectators. The state-of-the-art stadium is equipped to the highest standard including professional team facilities, a family area, corporate hospitality, a food village and world-class media suite.

With top-level professional rugby taking place at the ground and matches broadcast globally, Ulster Rugby looked to WiFi SPARK to provide a fully managed and supported Wi-Fi service that included a branded user experience portal, enhanced content filtering, bandwidth control, user data analytics and remote monitoring.

The use of the SPARK system which collects and analyses user data will permit Ulster to better understand the needs and requirements of its supporters. This insight will not only allow the club to enhance services but enable them to secure further sponsorship deals and revenue which can be ploughed back into the club for the benefit of its patrons.

Kingspan Stadium is the first stadium of its kind in Ireland to have this type of bespoke Wi-Fi solution installed. Supporters will benefit from a fully branded user experience, access to key information on what's happening in the stadium ahead of fixtures, and travel information to and from the stadium, as well as social media access throughout the grounds including during matches.

WiFi SPARK's experienced team of engineers has undertaken intricate installations across the globe and has a deep understanding of how the technology needs to be deployed in high-density, outdoor environments. Using this extensive knowledge and experience, Wi-Fi SPARK deployed the WiFi access points in precise locations throughout the Kingspan Stadium for optimal coverage and minimal interference, without compromising pitch integrity.

To cope with the sheer volume of supporters logging onto the Wi-Fi at the stadium entrances, Wi-Fi SPARK installed high-performance SPARK @ Gateways and high-density Ruckus Wireless technology, a proven combination. Each stand was simultaneously connected utilising a 10 Gigabit fibre backbone to the main gateways, providing high-density Wi-Fi access throughout the stadium.

Adrian McDonagh, IT Manager at Ulster Rugby, says: "We were really impressed by the technology offering from WiFi SPARK, and their consummate professionalism even in the face of a potentially problematic installation. With the excellent level of service they brought to the project, they are sure to be a key partner for us in the future."

# Delivering IoT safe city solutions

**Nick Koiza, head of security business at Plextek, looks at the drivers and strategies for delivering smart sensing in public safety**

The role of IoT in facilitating effective safe city solutions and supporting the work of the emergency services is currently in sharp focus. Here we look at and assess the key drivers and strategies for successfully delivering smart sensing solutions from a public safety perspective.

At every level of government, public sector organisations require access to increasingly large and disparate datasets. These datasets can relate to critical infrastructure, operational systems and citizens. From the perspective of real-time data access and dissemination, IoT safe city solutions offer significant value for improving public safety, services and long-term planning. For example, law enforcement, crime, traffic information, CCTV and facial recognition data provide valuable insights once captured, integrated and fully analysed. Such insights help to meet rising demand for improving public safety with increased efficiency.

The use of machine learning and artificial intelligence can be useful for reducing the level of manual analyses required on big data, preventing information overload and enabling fully-automated responses, based exclusively on key or critical information related to a potential threat or incident. Ensuring mission-critical information is instantly presentable to the right people at the right time and at the right place, will enable appropriate field staff and control room operators alike to enhance their decision making. With such intelligence to hand, public safety officers can act effectively on keeping smart cities safe and benefiting our communities by efficiently improving public safety.

## How to deploy

Recent developments in IoT have shown that effective smart and safe city solutions can typically comprise:

- Custom sensor devices deployed in the field and tailored to activate on certain triggers or thresholds, instantly alerting back-office or control room operator(s)
- IoT communications modules for relaying sensory information, for example, using NB-IoT or LTE Cat 1 or 4 for higher bandwidth applications – such modules are now widely available and represent important pieces of the jigsaw for creating devices
- IoT connectivity via an LTE network or low power local custom networks, as well as



*VAM systems enable the efficient management of vehicular fleets in emergency services, as well as heavy equipment and machinery, and also monitor driver behaviour for application in other markets, e.g., insurance. This is done through the incorporation of Cellular & PMR modems and GPS modules, which both need antennas to function effectively*

UNB (Ultra Narrow Band), LoRa, Sigfox, Zigbee and other systems. An IoT platform is necessary for real-time data management but also enables data mining when 'playing back' stored data for subsequent analyses. This is typically implemented in software and serves to provide a bridge between the radio and IT worlds. Additionally, a back-end IT application is required for an end-to-end solution, for example, within a control room environment where operators go about their duties. This includes monitoring operational intelligence from smart city devices or analysing and acting upon real-time alerts, or possibly performing some kind of field device reconfiguration or commanding activity, for example.

## IoT safe city solutions in action

Ambulatory electrocardiogram (ECG) monitors that record and transmit information from adult patients undergoing treatment to a hospital have now been developed and, having been approved by the Food and Drug Administration (FDA) in the USA, are currently being used in a third of all US hospitals. This is for ambulances to

better communicate with hospitals when a patient is being transferred to a health care setting and saves significant time in patient assessment on arrival if real-time data is coming from the ambulance in transit.

This new system obviously has to reliably transmit accurate readings of heart rate determination, R-wave detection, ECG filtering and arrhythmia recognition and this is done by incorporating multiple antennas, ensuring communication with patient-worn telemetry packs while en route. It means there is sufficient bandwidth to reliably monitor up to hundreds of patients at any given time.

## Fleet management and vehicle recovery for emergency services

Vehicle Asset Management (VAM) systems enable the efficient management of vehicular fleets in emergency services, as well as heavy equipment and machinery, and also monitor driver behaviour for application in other markets, e.g., insurance. This is done through the incorporation of Cellular & PMR modems and GPS modules, which both need antennas to function effectively.

For this, there is pressure to reduce the size of such products so they can fit into

often cramped conditions inside vehicles, which makes the development of antenna systems complex. To do this, the process takes account of the VAM placement inside the vehicle and the materials close to the unit, which may affect the performance of the antenna system. Using a custom-designed multiband-band cellular antenna integrated onto a PCB underlying layer, together with a custom GPS antenna, results in lower costs than equivalent COTS (Commercial off-the Shelf) antennas and enables integration into a tiny package.

Embedded tracking devices can be employed for stolen vehicle recovery and have successfully been used by luxury brands such as Mercedes Benz, while pothole detection systems are used by Jaguar Land Rover via the Synaptiv system.

## Police protection body armour

Body armour can be damaged during training or actual operations, resulting in its inability to provide adequate impact protection and decrease personal safety. Another issue is that the damage to the ceramic plates in body armour often takes the form of hairline fractures which are only visible during X-ray analysis, which are costly if done routinely.

The solution is an in-field integrity monitoring and testing sensor which can also be used within the defence and security markets. These sensors are low size, weight, power and cost and have a low training burden for users. It is done via a micro-electromechanical system with fine-tuned accelerometer sensors which detect shock waves associated with the formation of cracks caused by impacts. They also have a five year operating life from just a slim coin cell battery.

The solution also delivers the immediate status of the body armour to the user, removing the previous need for X-rays. It also means the user can rapidly assess the integrity of their body armour through status information presented as a simple, single screen graphic on a smartphone app, or by a press-to-test button showing a simple pass/fail via an LED indicator.

Of course, there are many more examples of emerging IoT systems which are and will transform the smart city environment and the work of the emergency services to make us safer. It is also expected that these developments will not only reside in urbanisations but migrate out to more rural communities in the near future.

## INDUSTRIAL IoT

### Connected Antenna Solutions

Reliable Antenna Solutions for Data Monitoring and Remote Control. 4G LTE & 5G-ready Cellular Solutions as well as Cellular/WiFi/GNSS Multiband Applications. Embedded, Fixed Site and Mobile Antennas.

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

www.MobileMark.com






# To break the energy curve with 5G, telcos are increasing efficiency by at least 10 times

Tu Jiashun, chief scientist, virtualization, ZTE

There is a growing concern in our industry around the environmental impact of our communications networks. These issues are not going away and as we move into the 5G era, the industry needs to act now to mitigate the impact of our energy consumption on the planet. 5G will see an explosion of traffic on our networks, driven by increased coverage, much faster speeds than ever before and the need to support massive IoT terminals and millions of connected objects. It has been predicted that total IoT connections on 5G networks could reach 1.35 billion by 2025. In order to break the energy curve, we must ensure that we lessen the environmental impact of our current network infrastructure and the networks we are building for the future will also be designed with these considerations from the outset. New technological developments are already making strides to address this and in some areas we have already seen a 10 times increase in efficiency between our 4G and 5G networks. In order to break the energy curve, network energy efficiency needs to increase up to 100 times in the long-term from what it is currently. Luckily there are a host of technologies that will help us reach this ambitious goal.

From streetlamps to flashlights, one technology that has seen significant investment in research and development is Massive MIMO. This technology is key to unlocking efficiency in 4G and 5G networks and is used widely in telecommunications infrastructure.

By way of an explanation, traditional base stations act a lot like a streetlamp. They emit a large signal with a wide radius and cover a lot of ground. The terminal that needs to access this signal only has one point of reception however. This means that the traditional base station is consuming large amounts of energy – much of which is wasted. Through the implementation of Massive MIMO however, you can turn that streetlamp into a flashlight, with a narrow and concentrated signal beam. This significantly reduces energy consumption while achieving the same signal level. Currently, Massive MIMO is perhaps the most advanced technology being implemented in an attempt to improve energy efficiency in telecommunications networks. It has been shown that it can improve efficiency by up to a dozen times that of a traditional base station. This technology has been implemented already on the 4G network but will also help to shape the next generation of telecommunications networks heading into the 5G era.

Another exciting area of development is in the arena of artificial intelligence (AI). It is still early days for AI and the technology's potential has been widely discussed in the technology sector for many years. We have already developed algorithms that are designed to monitor network traffic and make necessary adjustments in order to save energy. Traffic on the network is not constant and can dip or spike frequently depending on numerous factors. For example, during the day we experience far more network traffic than at night when some entire parts of the network can be shut down in order to save energy. This is one area in which AI has proven to be highly effective at cutting down energy consumption. Some algorithms have been developed to predict network traffic and match network capacity and performance to the traffic on the network at any given time. In Shandong, China, where this technology is already used commercially, AI energy saving solutions have led to a 150% increase in the power saved since its implementation. The energy saved across 10,000 cells at approximately 3,300

sites exceeded 21,000 kWh per week. This represents a reduction in carbon emissions of around 980 tons annually. Even more interestingly, this also resulted in major savings on electricity bills over the course of a year. The significance of this cannot be overstated. Only when organisations recognise that investment in green network solutions is commercially beneficial will we see the sort of sea-change needed to make a real and lasting change in our industry.

The green network revolution has already started and it is encouraging to watch our

industry wake up to the impact that we can have on our planet. To date, ZTE has applied for a total of 563 patents for green technology solutions. Of these, 146 are already operational and are currently being deployed not just in China but also in Europe and the United States. Innovation in this area will continue to be a priority of ZTE and other carriers in the industry. That said, we must not expect technological advances alone to be sufficient in making the necessary strides to a greener planet. The ongoing COVID-19 pandemic has highlighted the

need for us all to stay connected wherever we are and whatever our circumstances. This has, and will, continue to drive our society towards increasing digital communication. Our networks need to be able to support this. Parallel to this shift in how we communicate, we must also urge companies and individuals to explore new ways of working and living which focus on environmental consciousness. By pursuing this path, we are confident that working together as a society we can mitigate the damage to our planet.



PLUS  
Fully qualified  
NIC/EIC electrical  
engineers and  
in-house F-GAS  
certified engineers  
available

**ONE SUPPLIER...**  
Providing turnkey critical power solutions,  
including design, installation, maintenance & support

- Electrical installation & consulting services
- New thermal imaging capabilities
- Power ■ Cooling ■ IT infrastructure
- 3-Year warranty
- World class impartial advice saving you time & money
- Call now for a FREE site survey & health check
- Nationwide sales & engineering team, on hand 24/7

■  Installer

  
Design & Build

  
Cooling

  
Batteries & Accessories

  
Generators

  
Onsite 24/7 Services

  
UPS

  
Data Centres

  
Voltage Optimisation

  
PDU

  
Racks & Enclosures

**Critical POWER : When it matters most**  
www.criticalpowersupplies.co.uk | 0808 196 0370



# Choosing enclosures & containment systems

Michael Akinla, Panduit EMEA

**D**ata centre and enterprise computer room containment solutions (cabinets and enclosure systems, to you and me) are essential to the modern IT/Communications facility.

Today's increasing data throughput requires more complex and power-hungry processors and systems to cope with the user demand. The numerous cabinet product offerings from various manufacturers, may appear very similar, but understanding the development, testing, manufacture, product options and supply-chain can be the difference between a standard inflexible cabinet and a system customised and preconfigured to your precise requirements.

If you are the end customer or installer you need to be aware of the space to be occupied by the cabinets; ceiling heights, floor configuration – is it raised or slab – what equipment will be hosted within the cabinets, the power envelop per rack/cabinet and the installed technology's purpose and projected hosting plans for the next 5-10 years.

The equipment cooling strategy is

essential and a rule of thumb is 10-25kW (per rack), cold aisle containment (CAC), 25-40kW hot aisle/air containment (HAC), whilst above 45kW requires direct chipset cooling.

The next step is understanding the scope of the cabinets and enclosures within the white space. I recommend asking your cabinet or containment supplier, what level of design testing they undertake. Panduit has a state of the art 1600 square feet white space thermal lab, where we test and evaluate multiple-row cabinet layouts, targeting different containment solutions with various cabinets combinations and airflow delivery schemes. This capability allows us to recreate any floor layout and test for optimised design, which benefits customers in layout and cooling strategy and often eliminates redundant capacity in delivered solutions.

Among the benefits of grouping the cabinets together within a CAC or HAC solution are reduced costs, reduced energy use, and guaranteed cold and hot air separation and optimised equipment performance.

Power rating required by the servers

and communications equipment, and the cooling strategy for the room will affect containment and cabinet design. Equipment manufacturers' warranties now allow hotter operating environments, and so enclosures must be highly efficient in airflow movements to ensure maximum cooling is maintained. You should ensure the selected cabinets and enclosures provide air-flow calculations for the open apertures, such as mesh front and rear doors, whilst also offer gaskets and liners to seal possible air leak areas. Today's average rack power is 6kW, while many new applications require increased through-put and higher power requirement. A reduction in cooling airflow could result in an immediate increase in rack operating temperature which could trigger a processor shut down and possibly a more serious systems outage.

Sophisticated environment monitoring is now available for data centre environments including temperature and humidity sensors as well as magnetic door sensors for additional security.

To resolve problems such as integrating

upgrade cabinets with old solutions, ensure any shortlisted cabinet and containment system complies with Universal Aisle Containment format and offers features that make the deployment less costly and disruptive, and should include the following:

- Deployable as CAC (cold aisle containment) or HAC (hot aisle containment) solution
- Compatible with a variety of air delivery methods
- Ability to contain rows of cabinets of different heights, widths and manufacturers
- Ability to contain unpopulated or partially populated rows, without effecting performance.

As compute density increases pre-configured enclosures offering fully or partially complete racks and cabinets can be delivered direct to the customer. These plug-in solutions arrive complete with PDUs, standards-based cabling, connectivity, physical security and monitoring capabilities, reducing build time and increasing deployment speed on site, whilst greatly reducing packaging waste.

## PRODUCTS

**Schneider Electric** and Cisco bring to market a new pre-integrated edge computing solution, integrating Cisco's HyperFlex Edge, hyper-converged infrastructure (HCI) within Schneider Electric's "industry-first" 6U Wall Mount EcoStruxure micro data centre. HyperFlex is a com-



plete, engineered HCI solution built on the Cisco UCS platform, "enabling customers to extend the power and simplicity of HCI from data centres to critical IT systems at the edge of the network". Schneider Electric's 6U Wall Mount is designed for edge computing environments where space is at a premium and reliability is a must. It allows large, heavy edge servers,

networking equipment and UPS to be safely mounted on a wall. Consuming zero floor space, it is 60% less intrusive than traditional wall mount enclosures. Cisco certified shock packaging also enables channel partners and systems integrators to pre-install IT for quick and standardised deployments, with secure, ruggedised options for light industrial environments. The system is also fully compatible with Schneider Electric's next generation Data Centre Infrastructure Management (DCIM) software EcoStruxure IT, driving resiliency for distributed IT at the edge. [apc.com](http://apc.com)

**Eaton** reckons its RS Enclosure is a server rack available in network, server and colocation models to meet a variety of application demands. It says its versatile RS Enclosures offer everything from customisable and flexible mounting options for power equipment to high-flow doors for maximum airflow and a wide array of cable management options. [eaton.com](http://eaton.com)



**Excel's** Environ range of free-standing racks and open frames along with a comprehensive portfolio of wall-mounted racks is suitable for many applications in the enterprise, data centre and security markets, as well as for every day cabling systems. However, each rack family has been designed with specific applications in mind, helping customers to select the most suitable option for any installation. To complement the Environ range, Excel offers the Environ Locking Solution to provide an ergonomic and stylish



solution for environments where security is paramount. Bringing intelligence and monitoring right down to the lock level of a rack, the Environ Locking Solution provides ultimate access control. [excel-networking.com/environ-racks](http://excel-networking.com/environ-racks)

**Rittal** says its TS IT data centre solutions give IT users "unrivalled structure and support" through its flexible design and wide array of accessories. It says its TS IT racks offer an efficient internal space, variable widths and depths and baying versatility. Their standard parts allow users to configure solutions

that are tailored to individual data centres and allow for efficient cabling and thermal management (to protect sensitive electrical equipment from rising temperatures as the number of internal components increases). Meanwhile, the RittalXpress delivery service ensures that solutions arrive on-site quickly. [rittal.com](http://rittal.com)

**According to Corning**, its optical splice enclosures (OSE-RXD) are designed to help manage the transition between high-fibre count outside plant ribbon cables, such as the Corning RocketRibbon cable family and fire-retardant indoor cables in fibre optic networks. This, apparently, makes them ideal for use in data centre interconnect applications. The OSE-RXD was developed with simplified cable entry and management in mind to support reduced installation times for network applications with extremely high fibre counts. Unlike standard splice enclosures the OSE holds vertically integrated 288-fibre splice trays that allow for a single incoming cable leg length, resulting in ease of installation and enhanced time savings over traditional splice enclosures for the installer. The splice enclosure ships complete with splice trays providing capacity for up to 6,912 spliced fibres – or up to 13,824 with the RXD-HD – and all accessories for wall-mounted or 19-in equipment rack applications. [corning.com](http://corning.com)



**Siemon** says its new value vertical cable manager (VVCM) system simplifies deployment and the long-term management of critical network cabling infrastructures. The company claims it has been specifically developed to integrate with Siemon's 2-Post Value Rack, 19 inch Rack-Mount Horizontal Cable Managers and pathway support accessories to provide an equipment mounting and cable management solution that simplifies both the deployment and long-term management of critical network cabling infrastructures. Easily assembled in as little as five minutes, the new 7 inch,

45U vertical managers mount directly to Siemon's 2-Post Value Rack as well as other Siemon racking options, providing a cable management system that can be deployed rapidly. Available in widths of 4 inch (10cm), 6 inch (15cm), 10 inch (25cm) and 12 inch (30cm), the VVCMs are offered in both single and double-sided versions to enable a broad range of infrastructure topologies, simul-



taneously supporting cord management for high-density patching fields, efficiently routing horizontal cables, mounting PDUs, and routing equipment power cords. Unlike most vertical managers, which typically utilise difficult to operate snap-on covers, the Siemon VVCM line features dual-hinged doors with one-finger spring release clips at each corner. This user-friendly design

allows the doors to be opened in either direction to improve pathway accessibility and are much easier to open, close, remove, and re-attach than snap-on covers typically offered at this price point. The VVCMs also feature Siemon's unique, high-capacity cable management finger design. Capable of managing large quantities of larger diameter cable and cords in high-density environments as challenging as 48-port, 1U Category 6A patch panels, the fingers align with each U space, providing clear pathways for transitioning into the vertical cable management space. [ecatalog.siemon.com](http://ecatalog.siemon.com)





# “ Please meet... ”

Networking+ chats to Rick Goud, CEO & co-founder of Zivver

## What is the best thing about your job?

That I am able to be creative in solving the day-to-day challenges faced by people working in hospitals, governments and business in terms of effective but secure (digital) communication. Especially during Covid-19. This pandemic brings so many new challenges that we can overcome with the Zivver platform. Like now, we have just completed the rapid development of our technology to add secure video communication and enable secure digital questionnaires to be sent to healthcare patients via our platform. Shaping, designing, and developing these solutions really does give me a rush!

## Who has been your biggest inspiration?

That, I must say, is Elon Musk. Not that I like his management style, but he is a great inspiration when it comes to having an out-of-the-box idea, sticking to it and putting all you have into making that idea a reality. Time and time again. Really unprecedented!

## What is your biggest regret to date?

Thankfully not too many regrets. I am fortunate enough to have a great, healthy, family with three daughters, a beautiful house at the waterside - and working at my own company, with, now, 90 great colleagues, having thousands of great customers in essential and fascinating sectors such as healthcare, government, legal and insurance. What else could someone wish for?

## If you had to work in a different industry, what would it be?

I always wanted to be a doctor, since the age of four. But in the Netherlands there used to be a lottery system, where really you had to be lucky to get into med school. I was unlucky twice. I also liked medical informatics very much, so stuck to that. But sometimes, especially in these Covid-times, I have a small regret of not pursuing that dream...

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

I never really had heroes to be honest. Sometimes I hear my kids say 'Oh I would like to be this person (some Tik-Tok famous person?) soooooo much!'. I never really had that. I only had Baywatch-posters of Pamela Anderson and Yasmine Bleeth.... :)

## The Beatles or the Rolling Stones?

The Beatles. I can still sing along to most of their songs. My parents used to play them all the time in the car...those cassette tapes were played over and over again.

## What would you do with £1m?

Probably not much different from now. I enjoy my combination of work and family life very much. I'd probably give some to charity. Although I found out a couple of weeks ago that I already support 12 different charities with monthly donations of between 6-40 euros to each. So that was where my leak was :)

## Which rival do you most admire?

We don't have too many rivals. But sometimes people compare our proposition to Microsoft 365 (previously Office 365) DLP, encryption and privacy controls. And I must say that I

am very impressed with the changes Satya Nadella was able to initiate at Microsoft in terms of culture and proposition. Their shift to Office 365 a little under ten years ago really made their market leadership even greater – and it is probably here to stay.

## What's the weirdest question you've been asked at an interview?

No weird questions that I can remember - I like these questions though :) . Most interviews are quite similar, asking when and why Zivver was founded, and how, exactly, our technology

helps organisations to comply with the GDPR, DPA and other data protection regulations. From The Netherlands' healthcare-focused NTA 7516, to California's state-specific CCPA, I enjoy tackling questions on privacy standards as I'm a firm believer that people's data should be handled securely at all times, wherever they are in the world!

## If you could change any UK law, what would it be?

That digital communication would be obligatory instead of organisations using

faxes and letters for many purposes. Using digital communication only would improve costs, security and speed of communication so much! But who knows. Recently in the Netherlands, there was an emergency ordinance issued that all law firms and bailiffs are now obliged to use Zivver for communication, instead of using faxes and letters, for at least the duration of the coronavirus pandemic, as all the people working from home don't have faxes. Maybe other countries (and industry sectors) will follow soon!



## Connect USB devices to the network easily, safely and securely!



Questions? Interested in a test device? **Contact us!**

Phone: +44 (0) 1273-2346-81

Email: [info@seh-technology.co.uk](mailto:info@seh-technology.co.uk)

Made in Germany

### Features

- Isochronous USB mode: transfer of audio or video data streams
- Flexible and location-independent usage of USB devices in the network
- High performance device with 3 x USB 3.0 Super Speed Ports
- USB port 3 as charging port (e.g. for mobile devices)
- Fastest transmission of USB data from the USB device to client - up to 100 MB/s\*\*
- Enterprise security on both hardware and software levels
- Ideal for virtualized environments (Citrix Xen, VMWare oder HyperV)
- 36 months of guarantee (upgradable to 60 months) for free
- Free software updates, technical support worldwide
- For all common operating systems: Microsoft Windows, Linux, OS X/mac OS

### Areas of application



SEH Technology UK

Phone: +44 (0) 1273 2346 81 | Email: [info@seh-technology.co.uk](mailto:info@seh-technology.co.uk) | [www.seh-technology.com/uk](http://www.seh-technology.com/uk)