www.networkingplus.co.uk

OCTOBER 2018

networking

FIXED & WIRELESS NETWORKS FOR ENTERPRISE USERS

5G in the driving seat
Researchers send movie's worth of data in seconds to autonomous vehicle
News, p3

IT on the move
Network solutions for the travel and transport sector
Real World Networks, p8

Lock up you data
Some of the latest products and solutions to help secure enterprise data
Feature, pp10-13

Testing 1, 2, 3...
Test and measurement equipment. Plus buying advice
Off-the-shelf, p14

Emergency Services Network will now be launched in phases

The Home Office has decided on what it describes as a "new strategic direction" for the Emergency Services Network (ESN) which should have begun deployment last year.

In 2015, it was announced that the TETRA communications system used by the UK's emergency services and supplied by Motorola Solutions and Airwave would be replaced with a mobile-based communications network that uses LTE (*see News, January 2016*).

Rollouts were expected to begin in mid-2017, but in September, the Home Office announced that the project will now be launched in phases starting in the New Year.

The government said its new incremental approach means police, fire and rescue, ambulance crews and other users will be able to use data services over the network from early 2019, with voice capabilities following soon after. It added that it will also leave the emergency services free to test and choose which ESN products they want as and when they become available, rather than having to wait for the network to be fully implemented.

The Home Office is engaging with its commercial partners, EE and Motorola Solutions, regarding future changes to their contracts.

Separately, Motorola announced that its ESN agreement with the government will be extended by 30 months through the end of 2024. The agreement also includes extending the current Airwave network by three additional years to the end of 2022. As a result, Motorola said public safety organisations will be able to take advantage of the ESN's capabilities at their own pace while maintaining the Airwave network service to ensure uninterrupted service. The company will also upgrade the network.

Police, fire and rescue, ambulance crews, and other users will now be able to use data services over the ESN from early 2019, with voice capabilities following soon after.

As part of its delivery of ESN User Services, Motorola will implement a 3GPP standards-based push-to-talk software solution. This global platform uses technology from Kodiak Networks which was acquired by Motorola Solutions in 2017. ■

Businesses need clearer memories before disposing of old IT

Most businesses do not wipe the data from IT equipment they have disposed of, despite GDPR legislation that came into effect earlier this year in May.

After polling 1,002 workers in full or part-time employment, value-added reseller Probrand found that 68 per cent of businesses risk falling foul of the legislation by not doing so. It also reveals that 70 per cent do not have an official process or protocol for disposing of obsolete IT equipment, while 66 per cent of staff wouldn't even know who to approach in their company in order to correctly dispose of old or unusable equipment.

The top five industries that are most guilty of not zeroing the drives of redundant IT equipment include: transportation (72 per cent); sales and marketing (62 per cent); manufacturing (59 per cent); utilities (58 per cent); and retail (57 per cent).

Worryingly, Probrand says many companies in these sectors will have customer and client addresses and contact information on their systems.

"Given the amount of publicity around GDPR, it is arguably impossible to be unaware or misunderstand the basics of what is required for compliance," says Probrand marketing director Matt Royle. "So, it is startling to discover just how many businesses are failing to both implement and follow some of the simplest data protection practices.

"Given these findings, it is clear that more needs to be done to ensure that all businesses have a disposal procedure in place to avoid inadvertently leaking sensitive data."

According to the survey, other industry sectors that are guilty of not disposing of old IT equipment in a GDPR-friendly manner include: education; leisure and travel; health-care and hospitality; trades/administration; and information and communication. ■

The latest network security solutions – feature pp10-13

HE networks “more challenging” to manage

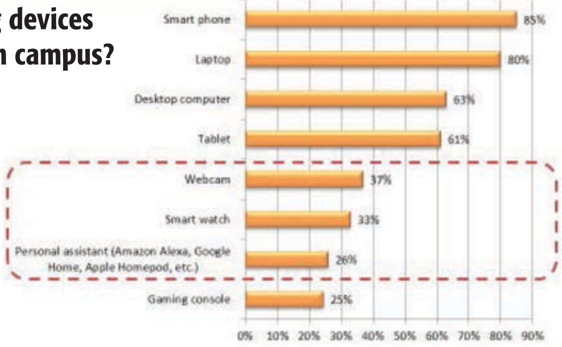
Networks at higher education institutions are increasing in complexity which makes them more vulnerable to attack, according to new research by Infoblox.

For its *Defending Networks at Higher Learning Institutions – Heroes Needed* report, the managed network services provider surveyed 678 students, staff, and IT professionals from HE institutions in the US, UK and Germany. It revealed that 81 per cent of IT pros believe securing campus networks has become more challenging in the last two years, particularly with the increase in the number of connected devices.

For example, while two years ago students mainly brought laptops and smartphones with them to college, the average student now brings in four or more devices (*see graph*). In addition, 60 per cent of faculty, students and IT professionals use four or more devices on the campus which drives up network activity.

IT teams are also challenged with a high volume of turnover in students each year when one quarter or more of their users change.

Which of the following devices do you own and use on campus?



The study found that compared to two years ago, there is now a “significant” number of new IoT devices used on campus networks.

SOURCE: DEFENDING NETWORKS AT HIGHER LEARNING INSTITUTIONS – HEROES NEEDED, INFOBLOX

Almost half of HE IT administrators believe the greatest security risks come from within the campus. For example, 54 per cent say at least a quarter of student devices come onto campus already infected with malware. Furthermore, 60 per cent of faculty and staff have not made any network security changes in the last two years, and 57 per cent use out-of-date security measures, such as updating passwords as a security precaution.

Infoblox found that lack of education on best practices is one of the major contributions to poor security hygiene amongst students and faculty staff. Thirty nine percent of IT administrators reveal that their users not being educated on security risks is one of their biggest challenges to keeping the network secure.

Beyond user error, outdated network technology poses another challenge. Seventy one per cent of students and staff revealed that their networks suffer performance issues at least once a month. Additionally, only 52 per cent of current network management solutions have DNS provisioning capabilities and can provide remote network access control.

“As higher education institutions embrace digital transformation and users become more device-reliant, their networks have become more complex and difficult to manage,” says Infoblox CTO of field engineering, Victor Danevich. “With this complexity, networks become more volatile and vulnerable to cyber attack if proper network security measures are not in place.”

The study also revealed that respondents from Germany’s HE sector were least confident in campus networks with 75 per cent noting they did not feel their personal devices were secure. That’s compared to 92 per cent in the UK. Here, respondents have the most trust in their students taking precautions to secure their sensitive data with 75 per cent trusting students. Meanwhile, only 47 per cent of those in the US felt the students were taking necessary steps. ■

Avanti cuts prices to help remote businesses get connected

Cornish businesses now have access to superfast download speeds of up to 40Mbps from less than £1per day by using the latest satellite technology. This follows Avanti Communications cutting the price of its European Regional Development Fund (ERDF) business satellite broadband scheme by an average of 63 per cent.

UK-based Avanti operates a fleet of satellites that covers Europe, the Middle East and Africa. Under a scheme financed by the ERDF, it provides subsidised superfast connectivity to rural businesses across Cornwall and Isles of Scilly. The initiative targets areas where there is no broadband connectivity or where access speeds are lower than 2Mbps.

Avanti is running the project from its satellite operations base at Goonhilly on the the Lizard peninsula. The project has funding to provide high-speed broadband connectivity of up to 40Mbps to up to 1,000 businesses across the region. It also covers a free satellite dish and a modem along with subsidised rates for installation and monthly tariffs.

Citing estimates from Cornwall Council, Avanti says around 6,500 businesses in the county are stuck in the “economic slow lane” without access to broadband speeds greater than 30Mbps. It says these firms communities have been underserved and are missing out on being able to grow their businesses. “They have not had access to the fundamental basics of being able to communicate with their customers and employees,” says Avanti’s chief sales officer Belinda Silous. “We are enabling Cornish businesses and entrepreneurs to have access to our superfast satellite broadband service to encourage growth in the [local] market [and] by delivering access no matter where they are located.” ■

Avanti is running the project from its satellite operations base at the famous Goonhilly site on Cornwall’s Lizard peninsula.

Connecting a remote coastal community in Scotland – News, p4.

Vodafone to double IoT network to expand enterprise possibilities

Vodafone will double the number of European cell sites in its 5G Narrowband IoT (NB-IoT) network footprint by the end of 2019.

It’s claimed this will create the world’s biggest, international NB-IoT network. It will be available in 10 European countries, including planned launches in the UK, Romania and Hungary.

According to Vodafone, NB-IoT is the ‘industrial grade’ LP-WAN (low power wide area network) technology that will provide connectivity for many smart city and industrial applications at low cost and with equivalent security to 4G. It says NB-IoT operates in licenced spectrum to guarantee customers service quality, provides “strong” coverage over large areas (even when devices are underground or deep within buildings), and provides “greater” power efficiency enabling devices to run on batteries for 10 years or more on a single charge. Vodafone adds that the technology also gives it the ability to support upwards of 50,000 devices in a single cell without congestion for the first time.

Vodafone IoT director Stefano Gastaut says: “NB-IoT gives businesses access to 5G capabilities a year before we expect large-scale consumer availability, and I believe this will be a catalyst in the widespread use of IoT by enterprises.”

Vodafone has already launched NB-IoT networks in the Czech Republic, Germany, Greece, Ireland, Italy, Australia, Netherlands, South Africa, Spain and Turkey. The company claims to be the global leader in managed IoT, with 74 million connections and an international network and services platform supporting companies such as Amazon, Audi, BMW, Bosch, Centrica, EDF, General Motors, nPower, Panasonic, Philips Lighting, Yamaha motorbikes, among many others. ■

Vodafone IoT director Stefano Gastaut claims NB-IoT gives businesses access to 5G capabilities a year before they actually become commercially available.

Paessler and Sigfox partner to accelerate IoT adoption – News p3

THE WORLD ACCORDING TO...

Alan Stewart-Brown, VP sales EMEA, Opengear

Cultivating long-distance relationships

The wave of transformation brought about by digitisation, the IoT, and decentralised hardware offers many efficiency benefits. However, these changes have created new challenges for centralised IT departments managing distributed branches, production sites and private clouds to avoid the consequential costs of network downtime.

Distributed networks are often more susceptible to service interruption and generally only larger branches will have an IT expert on site. With centralised monitoring and remote access to distributed resources, today administrators in many organisations can manage dozens or even hundreds of sites efficiently using in-band tools such as Telnet (teletype network). However, access is not possible during major technical issues such as network or connectivity failure.

In the legacy world, a remote failure would mean a technician has to go on site to resolve the problem that could range from a simple reboot to having to order a replacement device. The modern alternative to dispatching technicians is 'out-of-band' management that is independent of the function and connectivity of the local network which allows admins the ability to resolve issues remotely, to enhance resiliency and ultimately reduces downtime.

The principle is simple. Network attached devices are normally fitted with serial interfaces which can be interrogated independently of the network and give the administrator a complete picture of the status of the device. Many of the important management functions such as firmware updates are only available via serial console interfaces. If a device no longer responds to commands, administrators can carry out a hard reboot via the control system for the power supply.

Out-of-band management allows admins to maintain components such as servers, network devices and power supply units and resolve malfunctions via remote access. If there is an issue with connectivity, out-of-band solutions offer a failover solution that is often via cellular (4G LTE or 3G) or via PSTN modem for sites outside of coverage.

Out-of-band management has advantages beyond urgent crises. It also makes it possible to identify and resolve issues automatically even before they affect local data traffic using an autoresponder system to rectify network failures by using diagnostic and repair aids for problems that occur frequently. Increasingly, out-of-band devices are connected to local sensors to monitor temperature, moisture, smoke, vibrations and local power conditions for preventive maintenance and rapid incident response.

Paessler and Sigfox partner to accelerate IoT adoption

Sigfox has teamed up with network monitoring specialist Paessler to help customers more effectively monitor and manage their critical IT infrastructure and assets in the IoT.

As part of the partnership, Paessler has delivered its *PRTG Network Monitor*. Available in both hosted and on premise versions, Paessler's says *PRTG* enables IT administrators as well as IoT teams and integrators to see exactly what is happening in real-time across their infrastructure, including networks, systems, hardware, applications and devices.

Sigfox is using the system to visualise the functionality and measurement data from its IT infrastructure sensors, as well as from other objects, devices and machines that are equipped with or support its connectivity.

Paessler says the solution leverages two methods to initiate Sigfox messages to PRTG: callback, where data is sent immediately to the network monitoring system via push; and API, where PRTG requests data in predefined intervals from Sigfox connected devices.

The Germany-based vendor adds that "highly customisable" dashboards can be configured to show exactly what is important, from the overall health of the network, to granular details like the speed of fans in particular servers. *PRTG* generates alerts or notifications whenever any predetermined performance thresholds of the user's choosing are met, and also features the ability to automatically launch applications that provide a fix.

As part of the collaboration between both companies, Paessler is actively participating in the Sigfox Partner Network, while Sigfox is contributing to Paessler's recently launched Uptime Alliance partner programme (*see News, May issue*).

Sigfox's global IoT network is designed to connect billions of devices via its LPWAN (low power wide area network). This is expected to be available in 60 countries by the end of 2018.

"Our customers can virtually eliminate the overhead associated with connectivity, including the costs of the smart sensors and objects themselves," says Sigfox Germany CEO Vincent Sabot. "And with Paessler, our customers gain a single dashboard from which to monitor the connected devices and sensors that comprise their internet of things." ■

Scientists send a movie's worth of data in seconds to autonomous vehicle

Researchers at Warwick University's WMG research group claim to have set a new 5G communications speed record using a Level 4 autonomous vehicle. Working in the 28GHz millimetre wave (mmW) band, they are said to have hit 2.867Gbps in over-the-air transmissions. According to the team, that's nearly 40 times faster than current fixed line broadband speeds and equivalent to sending a detailed satellite navigation map of the UK within a single second, or an HD film in less than 10 seconds.

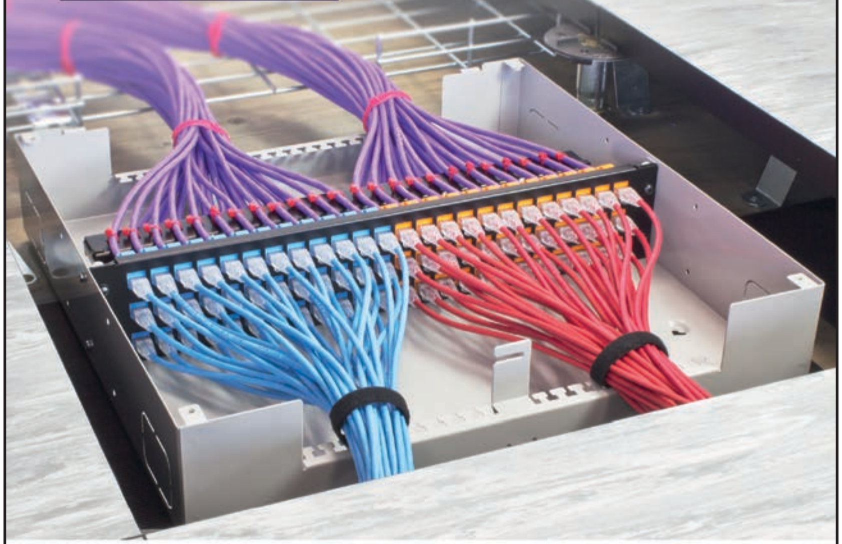
As well as being used to deliver high-definition content to in-car entertainment systems, the system will allow autonomous vehicles to rapidly share large quantities of data with each other and with traffic management systems. This will include precise 3D road maps created by LiDaR (a type of radar system that uses laser light instead of radio waves), HD video images of the vehicle's surroundings, and traffic information.

The WMG project's aim is to accelerate the introduction for connected and autonomous vehicles, and its facility at Warwick University is said to include some of Europe's most advanced 5G mmWave testing equipment. This has been provided by a £250,000 WMG Centre HVM Catapult award, alongside an equipment collaboration with National Instruments for its mmWave technology platform.

High-speed comms will enable autonomous vehicles to quickly share masses of data with each other as well as traffic management systems.

The research team set the communications speed record working with an autonomous pod built by Coventry-based manufacturer of Level 4 low speed autonomous vehicles, RDM. The team optimised antenna placement both inside the pod, and on roadside infrastructure, such as a traffic light.

WMG's Dr. Matthew Higgins says the controlled trials are critical to better understanding the capabilities of 5G in mmW bands. He says: "This project, which includes real-world 5G mmWave trials on the [university] campus, will also attempt to examine how the dynamics of both the vehicle and the environment affect performance between infrastructure and connected and autonomous vehicles." ■



EDITORIAL:
Editorial director: Rahiel Nasir
rahieln@kadiumpublishing.com
Designer: Alan McClenaghan
alanm@kadiumpublishing.com
Contributors: Matt Hodgetts, Paul Liptrot, Gerry Moynihan, Alan Stewart-Brown

ADVERTISING & PRODUCTION:
Sales executive: Andy London
andrewl@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
www.networkingplus.co.uk

Annual subscription: £80 (UK); £95 (Europe), £100 (USA and the RoW) airmail. Cost per single copy is £8.25.

Printed in England by
The Magazine Printing Company

KADIUM

CTS eyes growing European market with Qlouder merger

Manchester-based Cloud Technology Solutions (CTS) has merged with application development and machine learning specialist Qlouder. Financial terms have not been disclosed, and it's claimed the deal creates Europe's largest dedicated Google Cloud practice. The merger will see the creation of a 150-strong team offering expertise in app development, data science and machine learning. The business will operate from offices in the UK and Netherlands, enabling it to "significantly" expand its services across the continent. ■

Proact secures place on DOS3

Data centre and cloud service provider Proact has been selected to provide services as part of the Crown Commercial Service's latest framework, Digital Outcomes and Specialists 3 (DOS3). Under the agreement, Proact will offer a range of enterprise-class services to public sector organisations, including round-the-clock service management and security consultancy. DOS3 aims to support the delivery of the Government Digital Strategy. Under the Digital Specialists lot, Proact says organisations can leverage the "advanced expertise" of its cyber security consultants, data architects, data engineers and technical architects. Proact also provides public sector services through the Digital Marketplace on G-Cloud 10. ■

Claranet launches Global Cyber Security unit

Managed services provider Claranet has launched a Cyber Security unit to give customers access to its information security services. The firm says the move represents a consolidation of its current cyber security offerings following the acquisition and incorporation of Sec-1 and NotSoSecure into the wider group over the course of the last year. Sec-1's portfolio includes penetration testing and managed security services, while NotSoSecure is claimed to be the largest supplier of ethical hacking training courses to the Black Hat conferences. The launch of the unit is in addition to what Claranet describes as "considerable" investment in security services across its group operations, especially in France and Portugal. ■

Connecting a coastal community in Scotland

Rapier Systems has completed the installation of a new wireless broadband infrastructure to connect the entire Drimnin community in Oban, West Scotland.

The Fife-headquartered wireless networks specialist says it connected around 50 properties in the area, including homes, businesses and holiday lets, via licensed microwave links which its engineering team installed over the course of a month.

As a result, the remote, coastal community – which previously only received an average internet speed of 0.5Mbps – can now access speeds of up to 50Mbps.

Rapier used Cambium Networks' indoor *cnPilot R201P Wi-Fi* router which, as well as offering high capacity and fast installation, also enable remote access and management via an app. "This means we can fully monitor the network remotely and quickly identify faults if they arise," says Stuart Wilson, technical director, Rapier Systems. "We can also offer support to our customers quickly and avoid the costly and labour-intensive need for site maintenance visits. The remote access aspect was key to our success, as everything was able to be managed directly from our operational base."

Cambium claims its dual band *cnPilot* routers "streamline" components for a "simplified" indoor network. The company adds that they are backed by its *cnMaestro* cloud manager which offers end-to-end visibility of the network and customer devices.

Cambium Networks' routers are delivering speeds of up to 50Mbps in Drimnin. The firm reckons they're showing how fixed wireless access can help bridge the digital divide.

Drimnin is said to be one of Scotland's most remote places, located 12 miles away from Lochaline via a single-track road. It can also be reached by various ferry services. Cambium Networks' UK and Ireland sales manager Dan McCarthy says: "Drimnin is the epitome of rural areas in Britain which are underserved by traditional fixed lined access, and this deployment shows how fixed wireless access provides a cost-effective and fast means of high-speed broadband deployment." ■

TNP becomes Fortinet cyber security elite partner

Global cyber security expert Fortinet has appointed TNP (The Networking People) as a 'Security Fabric Expert Partner'.

Lancaster-based TNP focuses on high capacity users of the internet and networking across the public sector, including local government, healthcare and education. The company has developed what it describes as a "highly efficient and cost-effective" model that enables large organisations to design, build and operate their own networks independently of the established telecoms giants.

Fortinet Security Fabric aims to provide broad protection and visibility to every network segment, device and appliance, whether virtual, in the cloud or on premises. Many of the world's leading companies are said to rely on the fabric to segment their entire network and provide "superior" protection against sophisticated threats.

As well as being a Security Fabric Expert Partner, TNP is also a Fortinet Platinum Partner and claims this signifies that it delivers the "most advanced" levels of network security to customers. TNP commercial director Chris Wade says: "To cover today's attack surface, our company must demonstrate an ability to build a multi-layered security approach for the entire network, from IoT through to the cloud.

"As a Fortinet Platinum Partner, our staff are trained to deliver exceptional levels of service and able to confidently handle complex deployment requirements."

Wade also points out that the government's policy on cyber security stresses that users at all levels must ensure they are safeguarding their own systems. "Customers must therefore demand from their suppliers the highest levels of competence in the field of network and internet security," says Wade. ■

Clarification from the Data Centre Alliance

Following our September issue article about data centres (*'The centre of attention, pp11-13*) Steve Hone, CEO of the Data Centre Trade Association, has asked us to publish the following clarification regarding some of the points that were attributed to him:

"Whilst London is still a popular data centre location, the quality and quantity of power in the city is starting to become an issue, resulting in data centre providers opting to build further into the commuter belt. The attraction of these out of town locations is simple – lower land/real estate costs, and more power availability."

Hone points out that at any one time, the National Grid only has about three per cent capacity held in reserve, and while this has so far not led to brownouts, any unplanned strain on the grid – caused, for example, by a cold winter spike – could leave more than just the capital susceptible to unplanned power outages.

He continues: "Availability to international telco networks continue to make London popular in terms of a data centre location. However in general terms, with so much choice now on the outskirts of London offering both competitive pricing and the promise of higher power density per rack, it would be mad to automatically make a beeline to just Docklands unless your business needs absolutely demanded it.

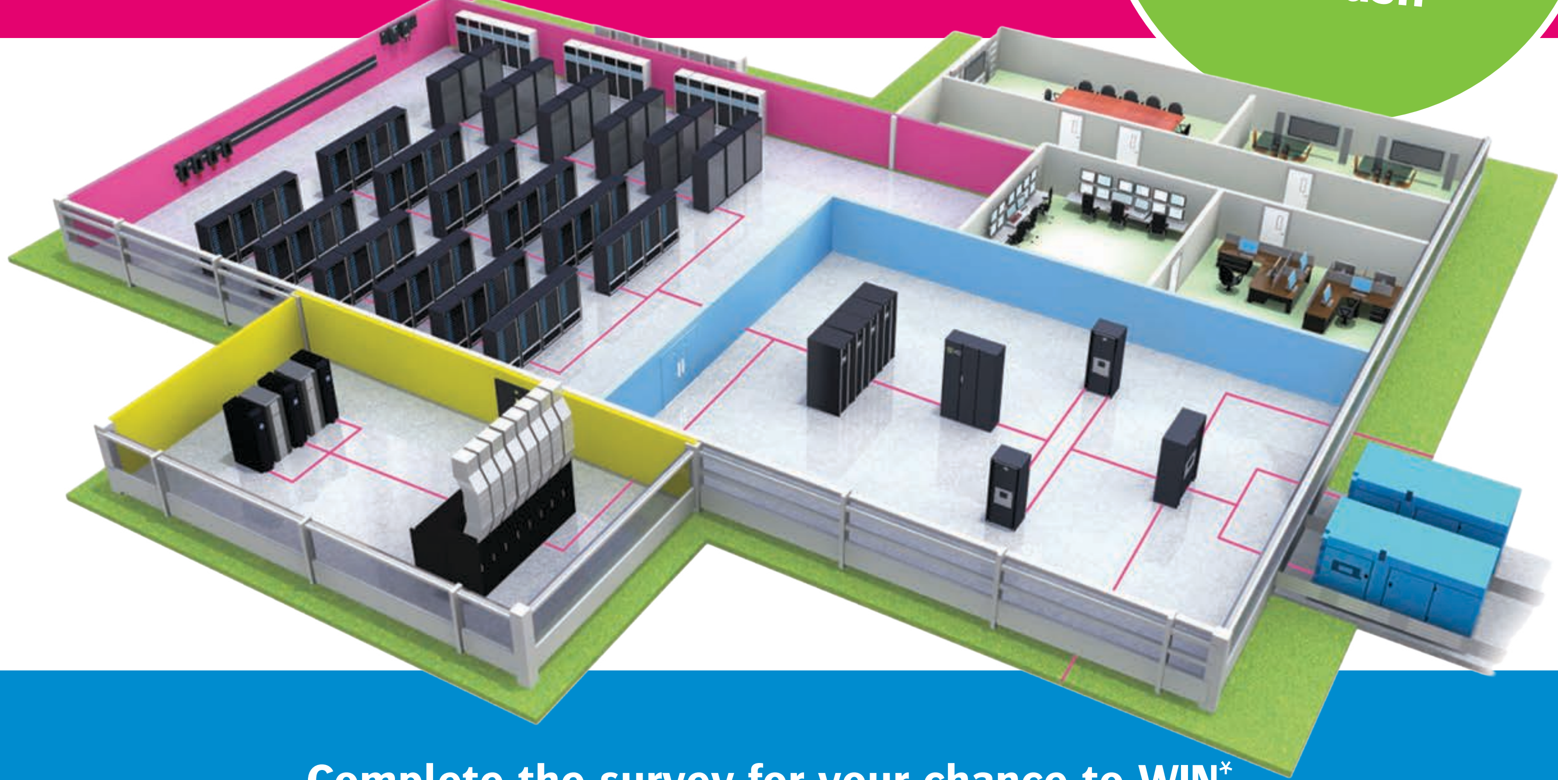
"Most data centre providers remain busy, but there are some who appear to be struggling. These tend to fall into two camps. There are legacy data centres who, despite operating good facilities, simply have too much space and not enough power to deliver the higher rack densities clients are now seeking. This can only be solved by giving them 200ft^2 of colo space just to host five 6kV racks – far from ideal.

"The second group who appear to be struggling are the single site operators who, despite having high quality facilities with all the power required, find it difficult to offer secondary facilities or backup/redundancy locations. To counter this threat, these independent operators have been partnering up so that they can offer the client an end-to-end solution and compete on a level playing field with the 'big boys' who already have multiple data centre location offerings." ■

Critical POWER
Supplies ▪ Projects ▪ Support

WIN a FREE data centre audit worth £10,000!

Trade in your old UPS for discounts or cash



Complete the survey for your chance to WIN*
a FREE data centre audit worth £10,000
The first 10 replies will win an APC Mobile Battery pack and one lucky winner will receive a £250 shopping voucher.
criticalpowersupplies.co.uk/forms/datacentresurvey

*Offer valid for all Networking+ readers until 30 November 2018. No purchase required. Terms & conditions apply.

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

Whether you're looking for construction, cooling, batteries & accessories, generators, onsite services, UPS, voltage optimisation, PDUs, or racks & enclosures, we offer:

- Three-year warranty
- World class impartial advice saving you time & money
- 24/7 nationwide sales & engineering team

0800 978 8988
sales@criticalpowersupplies.co.uk
www.criticalpowersupplies.co.uk

Multi-cloud adoption is a 'must' for enterprises

Report contributor Eric Marks says the multi-cloud ramp-up is a "wake-up" call for internal IT teams to "get their act together".

Organisations that delay multi-cloud adoption will become "increasingly irrelevant", according to a new study from F5 Networks.

In its *Future of Multi-Cloud* (*FOMC*) report, the cloud security and solutions provider aims to highlight game-changing trends and chart adaptive best practice over the next five years. The study was conducted by Foresight Factory which drew on its proprietary bank of more than 100 trends and original research across 25 regional markets.

Citing RightScale's State of the Cloud Report released earlier this year, the *FOMC* says 81 per cent of global enterprises claim to have a multi-cloud strategy in place.

"The multi-cloud ramp-up is one of the ultimate wake-up calls in internal IT to get their act together," says *FOMC* report contributor and VP of cloud consulting at CloudSpectator, Eric Marks. "One of the biggest transformative changes is the realisation of what a high performing IT organisation is and how it compares to what they have. Most are finding their IT organisations are sadly underperforming."

F5 believes new levels of service specialisation will increasingly allow enterprises to find the best tools for their specific needs, enabling seamless scaling and rapid service delivery innovations.

Its study says that the technologies set to drive this transition include serverless architectures as well as AI-powered orchestration layers, and configuration tools to aid data-driven decision-making. The researchers adds that fear of vendor lock-in is expected to continue as a key justification for multi-cloud investments.

The report goes on to caution that the multifaceted logistics of monitoring multiple cloud services, containers, APIs and other processes can be daunting and inhibit technology uptake. It says a significant skill gap also exists to handle this added complexity both now and into the future.

"Across the world, available workforces are not keeping with the pace of innovation, with potentially damaging results to business productivity and digital transformation capacity," states the FOMC. "Knowledge silos or lack of collaboration within businesses may further exacerbate multi-cloud apprehension." ■

The new managed service is said to help reduce the risk of shifting key business applications to the cloud.

BT first to offer Riverbed's Visibility solution 'as a service'

BT has become the first network services provider to offer Riverbed's *SteelCentral Visibility* solution 'as a service' to enterprises globally.

The new *BT Connect Intelligence Riverbed* Visibility-as-a-Service aims to give customers more timely information about how application data crosses their WANs. Riverbed claims it gives users "the most comprehensive, integrated and unified solution" for monitoring and managing the entire digital experience.

The platform is offered with three different service levels with what BT says is "simple, predictable and flexible" pricing options based on usage. It includes consultancy, reporting, design and implementation as well as global support.

The launch follows BT's integration of Riverbed's *Digital Performance Platform* into its network and cloud-operated service model. This allows the telco to offer *SteelCentral Visibility* capability as a service via its network to customers both in the UK and internationally where it is available in 89 countries. It includes a traditional hardware-based version of the solution as well as a VNF which runs on the *BT Connect Services Platform*. In both cases, BT offers a managed solution.

Neil Sutton, BT's VP of strategy and strategic alliances, says the new 24/7 service gives global enterprises a managed and cost-effective way to deliver the "very best" user experience as part of their digital transformation journey. He says: "It makes it less risky to model and adopt cloud and hybrid networks for key business applications, and helps customers implement new technology strategies such as Big Data analytics and IoT with confidence." ■

THE IoT CONNECTION

News & developments from the world of the Internet of Things. This month, we look at smart buildings.

Pangea and Buddy in UK power bid

IoT specialists Pangea and Buddy Platform are teaming up in a bid to transform the way energy is used in buildings in the UK and beyond. UK-based Pangea provides global IoT connectivity, systems, and actionable analytics. Users can remotely monitor, analyse, and control their networked devices via the company's portal.

According to Pangea, currently in the UK, 30 per cent of energy used in commercial buildings is wasted, 53 per cent of small businesses don't plan for energy usage, and 20 per cent of companies spend more than £250,000 a year on energy.

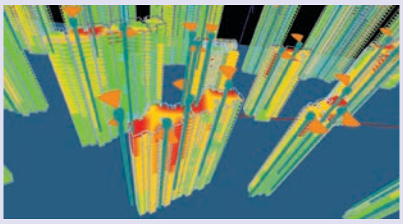
The company says that's where its 'Fitbit for Buildings' comes in. Through a combination of IoT sensors and SIM-enabled IoT connectivity, the device tracks a multitude of energy stats, all on a per building, floor, desk or device basis.

"It's more than just a tracker," says Pangea MD Dan Cunliffe. "The data collected helps your building tell a story of where and how energy is being used, and puts businesses back in control. Our goal is to address and solve a very real, tangible problem that every industry will face at some point."

Pangea says its system is installed in a few hours with a device that clips onto a surface in a building. This then communicates with Buddy Platform via Pangea's cellular IoT connectivity.

Headquartered in Australia, Buddy Platform has developed a number of smart solutions including *Buddy Ohm* which is at the heart of Pangea's 'Fitbit for Buildings'. Buddy claims its resource monitoring solution harnesses real-time utility and operational data to reduce or mitigate risk and improve operations, savings and sustainability.

Pangea says its system is installed in a few hours with a 'Fitbit' device that clips onto a surface in the building. This then communicates with Buddy Platform via Pangea's cellular IoT connectivity.



"Advanced" 3D visualisations and network propagation modelling will enable engineers to make immediate assessments and adjustments to indoor network designs.

Streamlining next-gen in-building network planning

PCTEL and Ranplan are promising to streamline in-building wireless network design, planning and optimisation with the integration of their software.

The companies say next-generation wireless networks will incorporate new technologies such as 5G alongside existing cellular, Wi-Fi, and public safety networks. By integrating PCTEL's *SeeHawk Touch* data collection software with Ranplan's Professional solution for planning, designing and optimising in-building and outdoor wireless networks in coordination, it's claimed onsite engineers will be able to measure, model and visualise the complex interactions between these technologies.

US-based PCTEL (Performance Critical TELecom) is global supplier of antennas and wireless network testing solutions. Its COO Rishi Bharadwaj says: "*SeeHawk Touch* and *Ranplan Professional* will enable network operators and building owners to prepare for a wide variety of uses, including emergency response, industrial IoT deployments, smart building automation and even virtual reality."

SeeHawk Touch collects and analyses real-world RF data from PCTEL's scanning receivers. *Ranplan Professional* then incorporates this data into what's claimed to be "advanced" 3D visualisations and network propagation modelling, allowing engineers to make immediate assessments and adjustments.

The companies add that the combined system will support network design and planning for a wide range of wireless technologies, including 3G, 4G LTE, LTE-A, CBRS, LAA, NB-IoT, Wi-Fi, P25, and 5G New Radio.

IX Reach brings cloud options to TeleData's Manchester data centre

IX Reach will provide cloud connectivity from TeleData's flagship data centre in Manchester offering tenants access to its full portfolio of services including direct connections into the cloud.

Cheshire-based IX Reach is a global reseller for internet exchange points and provider of wholesale carrier solutions such as remote peering, low latency point-to-point/multipoint capacity, cloud direct connect solutions, etc.

The company says it has partnered with TeleData due to demand for connectivity and access into the cloud around the North West. TeleData's independently owned and purpose-built data centre is located within two kilometres of Manchester Airport and 15km from Warrington where the chemical and pharmaceutical industries are prominent. Services offered at the 70,000ft^2 facility include server hosting and workplace recovery.

TeleData commercial director Matthew Edgley says: "Having IX Reach – who are official partners of *Google Cloud Platform*, *Microsoft Azure* and 'Advanced Tier' partners of AWS – present in our data centre will help the local economy and our tenants grow and future-proof their cloud strategies.

"Cloud connect also means any customer of IX Reach within other data centres will be able to connect privately and diversely into our own enterprise grade cloud solutions."

IX Reach adds that as well as being able to directly connect to the cloud platforms offered by Amazon, Google and Microsoft, TeleData's tenants will also be able to access more than 170 global PoPs, and all via what it claims is a "simple" cross connect. ■

IT on the move

Network installations in the transport sector must overcome their own set of obstacles.

No weekends off for installers at travel company

Each year, 6 million people take holidays with TUI UK & Ireland, part of the world's largest leisure, travel and tourism company. Its UK head office – a four-storey building in Luton – employs 3,000 of the company's 12,500 UK and Ireland staff.

With advances in technology, TUI needed a new IT network to allow faster applications, consistent Wi-Fi and to ensure an efficient and productive workplace. And it had to be installed while the building was open around the clock.

TUI chose Active Communication Company (ACCL), based in Orpington and headed by managing director Wayne Connors. Together, they decided that a new 10Gb network was required – with a new fibre optic backbone linking 20 network cabinets – to support all of the IT systems as well as building access control, meeting room system, Wi-Fi and CCTV.

ACCL decided to divide the project.

First, an eight-man team installed 8km of OM4 fibre optic cable over two weekends. Forty fibre cables were run under floors and above ceilings, split so that the whole network would never fail.

ACCL carried out an audit to create a clear plan because, it says, the existing network configuration had not been recorded and the cabinet cabling was disorganised with unlabelled cables.

TUI bought the 65 Cisco switches needed for the upgrade and ACCL built, configured and tested them off-site.

Over four weekends the team connected each of the four floors to the new network in turn, with TUI's weekend workers relocated to active network areas.

On Fridays, the ACCL team checked and removed the existing cabling, allowing the new cabling and switches to be connected the following day. The new cabling was carefully planned, labelled and documented, so any future changes would be simple.

On Sundays, all the IT equipment and other systems on the floor were checked. ACCL says careful planning meant that there were never more than three fault calls during Monday troubleshooting.

The general manager of technical services at TUI UK and Ireland, Scott Ronan, says: "Installation of our new network was an amazing piece of team work. To coordinate this work around other issues was challenging, but Wayne and the ACCL team were great."

Connors says: "This was a challenging project, both due to the technical aspects and the co-ordination required to maintain business as usual operations throughout. I am very pleased that everyone's hard work paid off."

Tunnel vision: how IT tracked big rail project

When Team BFK won three Crossrail contracts – worth a total of £700m-plus – the joint venture company decided to create a new IT infrastructure instead of using one from the three member firms.

Crossrail, which will be called the Elizabeth Line, is a 60-mile track, 26 of which are in tunnels, from Shenfield and Abbeywood to Reading and Heathrow. Priced at just under £15 billion, it includes 41 new stations and 30 upgraded stations.

Team BFK comprises BAM Nuttall, Ferrovial Agroman and Kier Construction. Its contracts consisted of two four-mile tunnels; access shafts and concrete lining at two stations; and a new station at Farringdon.

BFK decided to outsource the IT at the project office in Westbourne Grove and satellite offices. The tender was won by a Godalming company, Fordway Solutions.

BFK's head of business assurance, Geoff Bull, says: "Everything we do involves either communications or data storage, from working with our subcontractors, partners and Crossrail to the biometric site access management systems. As well as the typical office applications, we have applications such as AutoCAD for technical drawings, our planning and mapping software and our phone systems."

As well as linking the sites and ensuring continuity/disaster recovery, the supplier was required to configure all PCs and laptops, supply onsite and roving support and a 24x7 helpdesk. At peak, BFK had 700-plus staff.

BFK specified servers and data storage at Westbourne Park. However, Fordway's managing director, Richard Blanford, suggested using Fordway's own infrastructure in two UK data centres. It would save time, improve recovery and ensure the same level of service across offices. BFK agreed.

Fordway says it took four weeks to set up the infrastructure, including client devices and a fully managed, secure desktop service which included operating system and email management, email archiving, spam filtering and antivirus. It standardised on *Windows 7* and *Office 2010*.

Fordway says a "warm standby" service can bring all systems back online within 30 minutes. All services are charged on a cost per user, per month; BFK pays only for the capacity used; and the software is also on a rental model.

As the tunnel boring machines moved along, Fordway set up the IT in 23 temporary offices along the route. BFK is now gradually reducing capacity and Fordway is completing the archiving of all the project data as the contract comes to an end.

CCTV boosts safety for rail travellers

Each year, nearly 94 million passenger journeys are made on ScotRail trains. Since April 2015, the franchise has been run by Abellio, wholly owned by the Dutch national rail operator. ScotRail operates from 359 stations – 202 of which are unstaffed – with rolling stock totalling nearly 800.

In a move to reduce vandalism, make passengers feel safer and improve customer service, the company decided to add more CCTV and help points so that passengers could communicate directly with staff, even if the station was unmanned.

It hired Virgin Media Business to provide the leased lines which connect the stations to customer service centres in Paisley and Dunfermline and to install two Cisco LANs. The centres operate round-the-clock to monitor the audio and video feeds.

Staff also respond to passengers using the help points, often for train information and to report issues such as left luggage.

ScotRail reports a cut in vandalism, graffiti and crime at stations. ScotRail's communications and contingency manager at ScotRail, Anne Gray, says: "Many people who are on their own late at night find it reassuring to speak to someone and know that the operator can keep an eye on them until the train arrives."

In addition, the system allows operators to issue audio messages. Gray says: "We normally find that once we've given people an audible warning at the station, it registers and people don't offend again. It's a great way to get the message across, literally."

So far, more than 300 new CCTV cameras have been installed, with additional cameras monitoring cycle parking areas at 200 stations. Cameras and monitors have also been placed at the entrances to 30 of the network's busiest stations.

ScotRail says that 76 stations previously not covered by CCTV have seen it installed since the start of its franchise.

In a separate development, ScotRail reports a number of prosecutions using footage from body-worn cameras since they were introduced last year. Produced by an Edinburgh company, Edesix, they are worn on a voluntary basis. Each of the 300 cameras can record eight hours of high-definition audio and video which is downloaded automatically to a secure site.

They feature a 130-degree field of view, one-click recording and the ability to operate in low light.

A10 NETWORKS: FUTURE READY SECURITY SOLUTIONS

"Predict and prepare." These two words effectively encapsulate A10 Networks' journey in the world of cybersecurity. With the intuitiveness to predict the evolving threats and the ability to develop solutions to address them, A10 Networks has emerged as the cybersecurity vanguard, helping companies keep the threats at bay. Not to mention, the company is led by Lee Chen, CEO, A10 Networks, a visionary who warned that cryptocurrency motivated attacks would increase in 2018. While Chen's predictions have come true, his company is helping organizations tackle this menace by leveraging artificial intelligence (AI) and machine learning.

A10's cutting-edge security portfolio is geared to address more such threats in the wake of the digital

technology boom driven by cloud, IoT, smart cities, and mobile networks. Constantly updating its solution suite, the company empowers clients to be one step ahead of the cyberattackers. To elaborate, the recently introduced A10 DDoS Protection Cloud solution offers full-spectrum cloud scrubbing that improves the detection of malicious network traffic in the enterprise cloud network. Another recent addition to A10's solution suite is the One-DDoS Protection which efficiently handles threats with firewall and takes advantage of machine learning and AI to fight against new hacking methods that exploit bots. "Making sure we utilize cyber threat intelligence to tackle cyberattackers allows us to update our solutions faster," says Chen. A10 has a spectrum of solutions in its portfolio—all designed for every aspect of a business. Available in a wide range of form factors, A10's products can be hosted both on-premise and on the cloud for the most challenging network environments. The products can automatically defend applications and services in real time, even before advanced cyberattacks exploit them. In particular, the A10 Thunder product series has the ability to protect against sophisticated DDoS attacks and SSL visibility and decryption. It also offers secure application delivery and secures companies through converged, carriergrade, security best practices. In addition, A10 also provides Harmony Controller for improved data analytics and management, making it easy

for clients to protect their digital infrastructure by providing a single view of the entire network. Analytics solutions such as the per-app analytics available in A10 Harmony Controller empower companies to quickly and accurately detect security anomalies. The whole suite of A10's solutions is GDPR complaint. Alongside, A10 also has provision for companies to implement stronger identity hygiene practices like multifactor authentication to prevent attackers from breaking into the networks and stealing data. From firewalls to cloud scrubbing to A10 Harmony Controller, A10's solutions are designed to improve efficiency within the organization and allow IT professionals to focus on improving security and, in turn, business performance. For instance, SEGA Corporation, a video game giant, wanted to enhance its mobile game presence. They, however, required a robust and cost-efficient server to host the online abilities of their titles that could handle the high volume of traffic that SEGA was expecting. Implementing A10 ADC, SEGA gained high performance and usability through relevant traffic reporting options made available via local language GUI. With the recent introduction of improved ways to battle sophisticated cyberthreats, the first half of 2018 has been quite eventful for A10 Networks. The company believes that technologies like cryptocurrencies and 5G will gain tremendous traction, but there will be a simultaneous presence of threats. "We are working toward ensuring that our software is prepared for the large-scale attacks that might occur in future," concludes Chen.

Lee Chen, Founder & CEO, A10 Networks

The A10 Thunder 7445 Threat Protection System

A10 Networks Limited
Asmec Centres
Merlin House, Brunel Road
Theale, Berkshire, RG7 4AB, UK
Phone: +44 118 9026640
Email: EMEA@a10networks.com

Lock up your data!

With the subject of network security continuing to dominate the IT agenda, RAHIEL NASIR looks at some of the latest solutions to help safeguard enterprise data.

It is the number one topic in the IT industry: network security. Hardly a week goes by without splash headlines screaming about yet another data breach.

For instance, even as I write, the Information Commissioner's Office (ICO) has just fined Heathrow Airport Limited (HAL) £120,000 for failing to ensure that the personal data held on its network was properly secured. This relates to an incident in October 2017 when a member of the public found a USB memory stick which had been lost by a HAL employee. The stick, which contained 76 folders and more than 1,000 files was not encrypted or password protected.

ICO said that although the amount of personal and sensitive personal data held on the stick comprised a small amount of the total files, of particular concern was a training video that exposed 10 individuals' details including names, dates of birth and passport numbers, as well as the details of up to 50 HAL aviation security personnel. The stick was passed to a national newspaper which took copies of the data before giving it back to HAL.

ICO director of Investigations Steve Eckersley said: "Data protection should have been high on Heathrow's agenda. But our investigation found a catalogue of shortcomings in corporate standards, training and vision that indicated otherwise."

The investigation found that only two per cent of HAL's 6,500-strong workforce had been trained in data protection. Other concerns noted included the widespread use of removable media in contravention of HAL's own policies and guidance, and what ICO described as "ineffective" controls preventing personal data from being downloaded onto unauthorised or unencrypted media.

Heathrow Airport carried out a number of remedial actions once it was informed of the breach, including reporting the matter to the police, acting to contain the incident and engaging a third-party specialist to monitor the internet and 'dark web'.

Of course, HAL is not the only organisation to have been recently named and shamed by ICO. Boost Finance (trading as findmeafuneralplan.com), BUPA, direct marketing firm Oaklands Assist UK Ltd., credit agency Equifax, and marketing agency Everything DM Ltd., have all been hit with fines totalling £975,000 – and they were just for the months of September and October.

Most of the above incidents were due to sloppy IT security regimes rather than the result of a cyber attack. But even in the case of an external forced entry into their networks, enterprises need to make sure that they adopt a belt and braces approach to securing all data, or else risk ending up on ICO's penalties list.

The appliance of security

In an effort to stay one step ahead of the hackers, IT vendors have had to up their game when it comes to developing new products for safeguarding enterprise networks.

For example, Zyxel has recently released a range of firewalls that uses the cloud which is claimed to make "cutting edge cyber security simple" for SMEs. The company said its new ATP (advanced threat protection) line-up even defends against zero-day attacks that "fly under the radar" of conventional security solutions.

Designed as an all-in-one gateway solution, the new *ATP* firewalls feature several additional layers of security to detect and block threats. Chief among these is scalable, cloud-based sandboxing. According to the vendor, this executes unknown and potentially dangerous data packets in a safe, concealed environment to determine whether they should be let in or not. Zyxel said many threats don't make it to the sandbox. Like most security solutions, it says *ATP* assesses incoming data packets by checking the integrity of their signature. However, in addition to receiving regular updates of newly flagged signatures from trusted sources such as Bitdefender, the *ATP* firewalls also receive a continuous stream of updates for every new threat identified by every other *ATP* firewall worldwide.

For a complete solution that can neutralise threats in every form, Zyxel said the *ATP*s are fortified with six additional layers of protection. These include: web security (content and botnet filters); app and email security; intrusion detection and

Zyxel claimed its latest advanced threat protection appliances even defend against zero-day attacks that "fly under the radar" of conventional solutions.

Netgear's BR500 firewall can interconnect up to three offices as if they were connected locally, regardless of their geographical location.

prevention; geo-blocking; a managed AP service; and *SecuReporter*, an upcoming cloud-based service that analyses security data to offer insights that are said to be simple to understand and use.

There are two appliances available in the range: the *ATP200* offers throughputs of 1,800Mbps and is more tailored toward small businesses with one to 50 employees; while the *ATP500* is aimed at both small and medium-sized enterprises with up to 100 users and has a throughput of 2,600Mbps.

Netgear is also targeting SMEs with a router that it has designed for remote and site-to-connectivity while protecting digital assets in a single solution.

The *BR500* is said to enable small businesses or remote branch installations to offer instant access to the office intranet via a secure VPN from anywhere in the world. It is the first secure business router managed by *NETGEAR Insight* which enables remote employees to access data on their office networks with a single touch on a smartphone or a click on a laptop. *Insight* which is available as either a free app for *iOS* and *Android* mobile devices, or as a web portal accessible from any internet browser.

According to Netgear, the new device is designed specifically to enable businesses to instantly protect their networks with a secure VPN and firewall "rapidly and cost-effectively" through the Insight Cloud Portal or mobile app. It comes with easy setup, one-step 'Instant VPN', and anywhere remote/cloud monitoring and management.

The vendor adds that *Insight Cloud* enables full monitoring of all security features as well as remote management of the router, as well as enabling network managers to view real-time VPN connections and the security status of connected devices. As well as monitoring hardware status, temperature, port speeds, CPU load and memory utilisation, *Insight Cloud* can show the number of users connected to the VPN, their method of authentication, current traffic, visited destination from guest portal, sites connected (for site-to-site VPN), volume of data exchanged, and timestamp of the connection. It can also be used for firewall rule configuration and update, NAT traversal, port forwarding and FTP.

In addition, the *BR500* can interconnect up to three offices as if they were connected locally, regardless of their geographical location. Netgear said this makes connecting multiple offices for employees to share IT resources, such as file-servers, NAS or other business critical assets, easier, with users experiencing access to the local business network as if they were in the office.

Meanwhile A10 Networks has just released its *Thunder 7445 Threat Protection System* (*TPS*) with the promise of offering the industry's highest performance one rack unit and highest density of throughput per RU appliance. It claims the appliance offers 220Gbps throughput and 330Mbps.

A10 describes the new appliance as a "flexible and robust" DDoS protection solution that offers "surgical precision" in detecting and mitigating against the full spectrum of attacks. It says *Thunder TPS* provides a unique approach to full-spectrum DDoS defence, placing detection capabilities within targeted infrastructure, including its application delivery controllers, carrier grade networks and converged firewall solutions. A10 reckons this provides advanced context, flow and packet level visibility to stop today's most sophisticated targeted attacks. The company goes on to boast that the *Thunder TPS* delivers 6Mfps flow-based detection which is 22 times greater than the capacity of rivals, and can actively support up to 3,000 protected zones simultaneously which is claimed to be 15 times greater than traditional systems.

Other features include what's described as "automated wartime protection". A10 says this improves attack response times with proactive, intelligent automation featuring five levels of programmatic mitigation escalation and de-escalation. According to the firm, automated service discovery eliminates cumbersome manual provision and removes the need for frontline personnel to make time-consuming changes.

Always-on adaptive learning provides real-time adaptive traffic learning, with more than 27 tracked traffic indicators to eliminate detection errors. The appliance also integrates *Proactive Dynamic Attack Pattern Extraction* (*DAPE*) to thwart zero-day attacks.

In September, New Zealand-based Endace claimed a first with the launch of the *9200 Series EndaceProbe*. According to the specialist provider of high-speed network recording, traffic playback and analytics hosting, the new platform is the world's first petabyte network recording appliance. With built-in compression and patented technology that auto-truncates encrypted or non-compressible packets to maximise storage, it's claimed the *9200 Series* can record more than a petabyte of network traffic at a sustained 40Gbps.

In order to conclusively investigate and respond to security threats and performance issues, Endace believes many organisations rely on recorded network packet history. It said the new *EndaceProbe 9200 Series* delivers a 5x boost in packet storage density, "dramatically" extending the depth of network history that can be recorded for analysis.

The platform features new search algorithms that are designed to enable fast searching across multiple stacks of *EndaceProbes* and petabytes of network history. As a result, Endace said that security analysts can now find 'needle-in-the-haystack' packets in seconds rather than hours, anywhere on the global network.

Like all *EndaceProbe* analytics platforms, hosting capability is built into the *9200 Series*, allowing customers to host their choice of security and performance monitoring solutions from open source solutions, their own custom applications or Endace partners.

Earlier this year, G+D Mobile Security also claimed an industry first with the launch of a solid state drive with an embedded Secure Element (eSE) to store critical data. The German-based company said the product addresses the need for maximum, tamper-proof security of data stored on an SSD.

It features *CryptoCore SSD* which, says G+D, enables sensitive and confidential data to be stored easily and with the highest level of security. An eSE also ensures that sensitive data can only be accessed by authorised applications and people. *CryptoCore SSD* stores sensitive and confidential data on a tamper-proof chip embedded in the SSD. As a result, G+D said critical data are separated from conventional user data. It claims the risk of using 'infected' non-critical data to gain access to or manipulate security-relevant data is therefore "significantly reduced" without any extra effort on the part of the user.

G+D said typical users and applications that will benefit from its use are, for example, the health sector, aerospace industry, legal services such as lawyers and patent offices, as well as all other security-driven industries.

CryptoCore SSD is compatible with *Windows*, *Linux*, *MacOS* and various smartcard middleware products, and is a certifiable and standardised component. G+D said it can be retrofitted, centrally managed, and provides the ability to make regular and long-time updates of the eSE. This is said to lead to lower maintenance costs for IT security and

Endace said its 9200 Series can record more than a petabyte of network traffic at a sustained 40Gbps.

The A10 Thunder 7445 Threat Protection System promises the industry's highest performance one rack unit and highest density of throughput per RU appliance.

G+D Mobile Security's CryptoCore SSD is the first solid state drive with an embedded Secure Element to store critical data.

reduced total costs of ownership, while the system lifecycle is increased.

The SSD solution has a M.2 (Key B), a specification for internally mounted computer expansion cards and associated connectors. The interface is commonly used in industrial applications.

It is offered with G+D's *Sm@rtCafé Expert 7.0* JavaCard-based smart card OS which supports a range of crypto features such as AES, RSA, elliptic curves, and SHA 512. For increased robustness and protection against environmental influences, the modules are epoxy resin coated.

Black Box reckons its bringing to market new KVM switches with cyber security features that didn't previously exist. The US-based digital solutions provider – which describes itself as a "pioneer" in KVM technology back in the 1990s – said it now offers a comprehensive line of secure KVM switches that safeguard against accidental transfer, unauthorised access or compromise of critical data. It claimed the switches deliver peripheral access with "military grade" security against cyber threats.

The switches have been designed to provide complete mechanical, electrical and optical signal isolation to ensure that absolutely no data is leaked between the ports. Black Box said each connection uses its own isolated data channel to 'exclude' the outside world. For added security, the switches also feature an always-on tamper-proof hardware design, including external hologram tamper-evident seals and long-life internal anti-tampering batteries, along with keyboard/internal cache wiping and non-reprogrammable ROM.

All Black Box secure KVM switches comply with PSS PP v3.0 (Protection Profile for Peripheral Sharing Switch) and are certified by the US' National Information Assurance Partnership.

Black Box reckons its new KVM switches deliver peripheral access with "military grade" security against cyber threats.

Cloud cover

The issue of security hindered adoption of cloud services during the early days. But many of those fears have now been laid to rest and cloud migrations have been ramping up – according to research conducted by the Cloud Industry Forum last year, the UK's overall cloud adoption rate currently stands at 88 per cent, with 67 per cent of users expecting to increase their adoption of cloud services in 2018.

As a result, many specialist vendors of software security have been focusing on developing products that specifically target cloud security. For example McAfee has just unveiled two new products expanding its *MVISION* portfolio which, said the firm, is "a first-of-its-kind solution that allows customers to deploy security on their terms as they move to the cloud".

The new products include *MVISION EDR* (endpoint detection and response) which has been designed to enable security teams to act faster and with higher precision so they can do more with their current staff and skill sets. According to McAfee, many organisations typically suffer from "information overload" when it comes to most EDR systems. It said this is because such systems generate volumes of data and alerts that require skills – that are often in short supply – to interpret and investigate before action can be taken.

It's claimed *MVISION EDR* implements human machine teaming to enable analysts of all skill levels to be more effective and efficient. It is said to utilise "advanced" analytics that leverage Mitre's *ATT&CK* framework to identify and prioritise suspicious behaviour from contextually rich endpoint data. McAfee said these analytics help guide and automate in-depth investigations to reduce the tactical strain on security analysts, and enables rapid response with direct actions and broader integration to the security ecosystem.

The second new offering is *MVISION Cloud*. McAfee said that as information moves from protected on-premises corporate networks to the cloud, it can be very difficult for organisations to secure both sanctioned and unsanctioned services, protect sensitive data across the cloud, and stop the most advanced threats. The vendor reckons it has solved this problem with *MVISION Cloud*. It said this offers centralised management and brings together data protection and threat prevention across public cloud services spanning the SaaS, IaaS and PaaS spectrum

MVISION Cloud is designed to provide visibility and control across all cloud services. It uses a combination of API- and proxy-enabled approaches, with DLP policy that can be extended from devices to the cloud. McAfee said this includes content scanning, logging and activity monitoring and threat and malware detection. It added that the new platform protects against malware and external and insider threats through UEBA (user and entity behaviour analytics) driven by machine learning built for the scale and elasticity of cloud environments.

Earlier this year, cyber security and application delivery services specialist Radware launched its *Cloud Malware Protection Service*. The company said this has been built to detect, alert and block zero-day malware that eludes existing anti-malware defences and steal data.

The new cloud-based service includes audit tools that continuously test the user's network for gaps in malware protection, as well as real-time reporting to help organisations comply with GDPR and other regulations focused at private data protection. It relies on traffic analysis to detect communication anomalies indicative of evasive zero-day malware activity. Radware said its service leverages "advanced" machine learning, patented algorithms, Big Data analysis, and a global community of more than two million enterprise users to identify and block malicious traffic that is consistent with data theft.

Cloud networking provider Aerohive made its entry into the secure access market earlier this year with the launch of A^3 which is billed as the industry's first hybrid cloud-access management solution. The authentication, authorisation and accounting (AAA) platform is said to offer a comprehensive portfolio of access-management functionality to enable onboarding and security for IoT, BYOD and standard wired and wireless clients. Aerohive reckons A^3 delivers a complete, secure access solution, such as automated device provisioning, device profiling and network access control, self-service onboarding, and even guest access. It added that all this is done without the "operational complexities" associated with rival offerings.

A^3 aims to deliver a complete, integrated cloud product for effective network security and client management, combining streamlined workflows, an "intuitive" UI, and what Aerohive said is its "cloud networking competency". It is designed to be compatible with network equipment from all major vendors, but is said to feature unique, value-added functionality when deployed as part of an Aerohive SD-LAN/SD-WAN platform. These include, for example, integrated private pre-shared key (PPSK) management as well working with the vendor's *HiveManager* management platform.

Aerohive believes its solution is also unique in its ability to be deployed on-premises, akin to more traditional AAA and access management solutions. It will also be available as a cloud service accessible from the *Aerohive Cloud Services* platform. The company adds that it will be possible to configure a combination of the two, with certain functions distributed to remote premises and others centrally managed from the public or private cloud.

Privileged access management (PAM) company Bomgar has now completed its acquisition of BeyondTrust (*see News, September issue*), and says the integration of its remote access solutions with BeyondTrust's PAM platforms will allow users to authenticate to a managed device and logon without ever knowing the credentials or assigned privileges of the devices they are accessing. "Essentially, their identity will translate from remote access seamlessly through privileged access to any target that they have permissions to access," said Bomgar.

Prior to the merger of the two companies, BeyondTrust announced what it said was a first-of-its kind privilege management solution for network, IoT, ICS and SCADA devices. *PowerBroker for Networks* expands the company's privilege management support which includes Windows, Mac, Unix and Linux endpoints, servers, applications, and now any device managed via SSH or Telnet. BeyondTrust claimed that by using the product, customers can realise the benefits of end-to-end least privilege "faster and with less complexity" across nearly all environments, including critical network devices.

PowerBroker for Networks is an agentless solution that controls what commands users can run, records sessions, alerts, and provides a complete audit trail of user activity on network devices via the command line. Since most network devices do not allow for the installation of agents, or are manufacturer-specific, BeyondTrust believes its solution fills an important gap.

Delivered with a modular design, *PowerBroker for Networks* features is said to "easily" scale to hundreds of thousands of nodes without overburdening the network or administrators with overhead. BeyondTrust said organisations can manage large, distributed, and heterogeneous infrastructures while delivering optimal performance and without limiting activity. The firm added that the solution fully integrates with the central *PowerBroker* console, enabling customers to benefit from a single policy, management and reporting interface.

Because the software supports any device that utilises SSH or Telnet to enable management, BeyondTrust said it can be utilised across a diverse network and offers a number of features. These include enabling full, granular control and auditing of all commands and sessions to network devices. Real-time session monitoring warns, or warns then terminates, a session when questionable user behaviour is detected. *PowerBroker for Networks* also integrates with security information and event management (SIEM) solutions for complete security intelligence, generating logs and sending them to syslog to be picked up by a SIEM system.

Other features include alerts to prevent or stop unwanted activity for faster cyber security response, integration with password management solutions such as *PowerBroker Password Safe* to seamlessly retrieve passwords for automated sign-on through a proxied connection, and centralised control of policy and audit data for decentralised devices and administrators.

Speaking at the time of the launch of *PowerBroker for Networks earlier this year*, BeyondTrust COO Brad Hibbert said: "Network devices – such as routers, switches, firewalls, IoT, ICS, and other SCADA devices – are critical for organisations to function, yet present open doors for external attackers and malicious insiders if not properly monitored. To improve security on these devices, organisations must have control and visibility over privileged user activity."

Bitdefender has come up with a complete endpoint prevention, detection and response platform aimed at all organisations. Called *GravityZone Ultra 3.0*, it is said to be the industry's first single-agent, single-console endpoint protection solution to combine prevention and hardening with "advanced" EDR.

Like McAfee with its *MVISION* portfolio above, Bitdefender also believes that EDR systems have proved challenging for users to deploy. According to the firm, enterprise adoption of such solutions have so far been limited due to "the realities faced by today's, resource-constrained security teams trying to manage large volumes of security alerts with disparate, marginally integrated solutions".

Bitdefender's GravityZone Ultra is designed to simplify deployment and operations across all enterprise endpoints, including Windows, Linux and Mac OS, in physical and virtual infrastructures, and across data centres and public cloud environments.

To solve these problems, Bitdefender said it built *GravityZone Ultra* from the ground up to help to help organisations coping with complex infrastructures by keeping protection, detection and response manageable. It has been designed to eliminate the need for multiple agents, simplifying deployment and operations across all enterprise endpoints, including *Windows*, *Linux* and *MacOS*, in physical and virtual infrastructures, and across data centres and public cloud environments.

GravityZone Ultra works as a single, homogeneous solution with integrated workflows and advanced forensics. All this is said to, enable IT teams to effectively deploy and seamlessly manage EDR as a new layer of defence in concert with the platform's prevention capabilities.

According to Bitdefender, IT organisations can now use advanced EDR features such as pre- and post-compromise forensics, intelligent scoring of suspicious activity, attack-technique visualisation, real-time Indicator-of-Compromise (IoC) search, and automated resolution, all from within a single platform. This is said to help administrators identify incident origins more quickly, and uncover and close vulnerabilities across the organisation. Bitdefender claims new real-time and historic IoC search using natural language queries enables administrators to efficiently target and disable threats on any platform. It added that visualisation of attack techniques based on Mitre's adversarial tactics, techniques and common knowledge tags are used to identify traces of attacks or suspicious activities, while an intelligent, automated 'Severity Score' dramatically reduces the overhead that plagues other solutions.

The company continued by saying that by combining *GravityZone Ultra*'s advanced prevention capabilities and its new features with attack timeline and sandbox output, threats are either blocked or incident response teams are able to react quickly to stop ongoing attacks before they do damage. This further protects and closes the loop for enterprises in their daily battle against sophisticated cyber threats, vulnerabilities and risk exposure. ■

Putting your network installation to the test

Some of the latest test and measurement tools to help ensure your network makes the grade. Plus, MATT HODGETTS offers expert guidance about what to look for before renting test equipment.

Whether you're working on a short-term project or designing a leading edge system and need to easily refresh equipment to maintain competitive advantage, the decision to rent test equipment can be straightforward. But there are other considerations many engineers don't think of prior to doing this.

To help make sure you're prepared for your next equipment rental, Microlease's application engineers have pulled together this unique checklist of top tips:

1. Do you have the complete test solution?
When looking for equipment, such as a network analyser, you may not think to ask for cables, connectors, calibration kits or other ancillary items that will be required. If these aren't included in the original order, it could take another week to get them, making those deadlines even more stressful.

2. Will your equipment need calibration?
Rentals can mean no more calibration and maintenance worries or costs. Also, if something changes you can get upgrades and support. If your equipment will need calibration before and/or during your rental, make sure your rental company can calibrate to the standards you require (for example, Ansi Z540 and ISO 17025).

3. How long will you need the equipment?
Rentals and short-term projects go hand-in-hand, but sometimes you may not know just how long you will need the equipment. With rapidly advancing technology, odds are that the advanced test equipment you need now will be obsolete within one or two years. A flexible rental offers the ideal solution with rental periods from just one week to as long as you need.

4. Do you need the equipment locally or globally?
You may only have one local site for testing or you may have multiple labs working on designs in various parts of the world. It's important to make sure the company that you're renting from offers the geographical coverage you need to ensure you get the equipment on time and with good backup service.

Matt Hodgetts is a sales engineer at Microlease UK. www.microlease.com/uk/rent-test-equipment.

New handheld fibre testers from **Anritsu**, the *Access Master MT9085* series, have an 8in colour touchscreen and include the company's *Fiber Visualizer* as standard.

Anritsu says the screen, rotary knob and hard keys improve OTDR waveform analysis for ease of use, helping to reduce time on site. And, it says, *Fiber Visualizer* also saves time as well as simplifying verification.

According to the company, field technicians can use the tool to display fibre events, such as splices, connectors, and splitters, as a schematic map. By eliminating complex operations, such as reading and analyzing optical waveforms, it allows technicians of any experience to carry out high-quality fibre measurements and pass/fail evaluations. Also, automatic pass/fail evaluation based on preset threshold values reduces evaluation errors.

In addition to a fully-featured OTDR, the *Master MT9085* series can conduct optical power loss measurements and fibre far-end detection. It is designed with an algorithm which is claimed to detect fibre events with high accuracy in complex passive optical networks (PONs).

Anritsu says it features high-speed, high-quality real-time waveforms, short dead zone of ≤8m, high dynamic range of ≥46 dB, and support for both single-mode optical fibre (SMF) and multi-mode optical fibre (MMF) waveforms.

Technicians can now be freed from the buzz from external sources when testing cables, says **Fluke Networks**. It has introduced the *Pro3000F Filtered Probe*, the latest in its *Pro3000 Tone* and *Probe* range, which has a filter that removes signal interference at 50 or 60 Hz and their harmonics.

This filtering, the company says, allows technicians to easily find the cable or wire they are tracing even when noisy external sources, such as power cables and lighting, are present. The company says the filtered version was the most requested enhancement by its customers.

According to Fluke, technicians find that in certain environments, such as a building renovation, sources of signal interference including power tool power supplies, lighting and fans can overwhelm the tone being sent by a standard tone generator.

This noise usually has a frequency of 50 Hz or its harmonics – 60 Hz in north America – which can hinder the technician's workflow or make it impossible for them to trace cabling accurately.

The *Pro3000F Filtered Probe* is sold separately or with the *Pro3000 Tone Generator*, which features *SmartTone* technology that provides five distinct tones for exact pair identification.

Touchscreens have been added to several of **Ideal Networks**' network and data cable testers, designed to make troubleshooting and transmission testing quicker and easier.

Following the upgrade, a 240x320 pixel LCD capacitive touchscreen is now standard on all new *NaviTEK NT Plus* and *Pro* copper and fibre network troubleshooters, *SignalTEK CT* data cable transmission testers and *SignalTEK NT* network transmission testers.

Ideal says all the new touchscreen models enable fast and responsive data input, making it quicker to type in names and other data. It says that, like a smartphone or tablet, the capacitive screen is tough yet sensitive, ensuring only a light touch is needed to operate the onscreen keyboard. It points out that many technicians and installers often use touchscreens on other devices, so the upgrade offers a more intuitive way of working, helping to save time and increase efficiency.

As well as touchscreen operation, the upgraded testers provide a choice of ways to enter data. If preferred, says Ideal, the onscreen keyboard can be operated using push buttons on the handset, a benefit to those wearing gloves – there is no need to remove them to enter data.

When users complain, engineers can be overwhelmed with sifting through a sea of KPIs to deduce exactly what users experienced, says **Viavi**. And it says it can be even more confusing when problems remain while all the indicators show green.

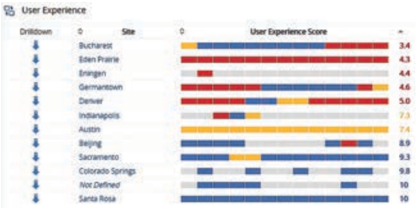
It quotes Forrester Research as saying one-third of user complaints linger without resolution for a month or are never resolved.

Viavi says that, armed with only a one-dimensional view based on network performance data, IT support teams have to make rough guesses at the cause of user experience issues, wasting time and money.

The company says that the latest in its Observer range, *Observer 17.5*, turns performance monitoring on its head by integrating intelligent end-user experience scoring with workflows for any transaction.

Viavi's "End-User Experience Score" uses adaptive machine learning to run hundreds of data sets through an algorithm to output a single score which indicates where the problem is with a simple problem explanation along with performance visualisations.

As a part of investigative workflows, engineers can quickly solve any issue and provide filtered wire-data evidence to IT teams. And Viavi says that Observer provides full-fidelity forensics for performance and security in high throughput networks with interfaces for 1/10, 40, and 100Gb.



User Experience

Drilldown	Site	User Experience Score	
⬇	Bucharest		3.4
⬇	Eden Prairie		4.3
⬇	Erlangen		4.4
⬇	Germantown		4.6
⬇	Denver		5.0
⬇	Indianapolis		7.3
⬇	Austin		7.4
⬇	Beijing		8.9
⬇	Sacramento		9.3
⬇	Colorado Springs		9.8
⬇	Not Defined		10
⬇	Santa Rosa		10

The cyber card game is said to offer a proven and more enjoyable approach to cyber training.

Dstl develop cyber security training game

Scientists at the Defence Science and Technology Laboratory (Dstl) have developed a cyber card game that claims to "fundamentally alter" the way cyber is thought about, taught and employed.

According to Dstl, cyber threats are varied and often very sophisticated, meaning they may go unnoticed. It adds that training staff to recognise and counter common information warfare attack strategies can be difficult, time-consuming and expensive.

Dstl scientists claim their card game provides "rapid upskilling" in understanding high level, open source cyber attack techniques, and enhances learning on possible defensive strategies. They say it offers a more enjoyable approach to cyber training with staff having the option to continue playing in their own time.

The game is also designed to be adaptable across a range of audiences and knowledge levels. Dstl says it can be tailored to various scenarios, ranging from a rapid two hour session for corporate management through to an extended campaign for cyber professionals. Furthermore, it avoids using classified information and therefore does not need security clearance to play.

Dstl says extensive testing of the game and positive stakeholder feedback has shown a very rapid initial learning curve compared to conventional training alone. It is now available for license on a non-exclusive basis through the lab's Easy Access IP licencing framework. This enables companies to develop Dstl's work at no cost, facilitating commercialisation of products that will benefit the economy and society.

The first licencing agreement has been signed with Coruscant Productions which plans to develop and market the cyber card game training approach further. The company's founder Tomas Owen says: "The cyber card game fundamentally alters the way cyber is thought about, taught and employed."

RGU offers free courses to help address skills shortage

Aberdeen's Robert Gordon University (RGU) is hoping to help tackle the widespread skills shortage in the IT industry with the introduction of fully funded places on its suite of MSc computing courses.

In addition to places on its specialist *Cyber Security* and *Computer Science* masters programmes, RGU also made free places available on a range of IT MSc courses that are suitable for graduates of non-computing disciplines. These include: *IT*; *IT for the Oil and Gas Industry*; *IT with Cyber Security*; *IT with Network Management*; and *IT with Business Intelligence*.

In 2016, ScotlandIS – the organisation representing Scotland's IT sector – estimated that the country would need at least 11,000 extra ICT workers each year for the next five years. However, there are only 2,000 ICT graduates per year from Scottish universities.

John McCall, head of RGU's School of Computing Science and Digital Media, says the skills deficit is detrimental to the growth of digital economies and that many firms are struggling to recruit workers they need. He says: "It is widely acknowledged that there is a huge shortage of people who are highly trained in IT and who have the skills and knowledge to address a lot of the challenges that business, government and commerce are facing nowadays in relation to [Big Data], cloud computing and web systems.

McCall claims the university's courses aim to address this and will produce graduates with the advanced skills needed by industry and commerce for both today as well as the future.

IN BRIEF...

■ Rittal has developed two new accredited seminars. *Challenging 'The Edge' – IoT* considers how the growth of cloud storage, alongside the need for higher speed and low latency, has fuelled Edge Computing to support new technology such as 5G, as well as the rise in video content, and machine-to-machine learning. The second seminar, Open Compute *Project & Open19 Project*, explores the Open Compute Project (OCP) which was launched by Facebook in 2011 to share knowledge about building low-cost, highly efficient data centres, particularly those used by hyper-scale cloud platforms. Alongside this is LinkedIn's *Open19* project which is aimed at data centre operators who are smaller in size but which house the majority of the world's IT infrastructure. The seminar explores Open19 hardware which is built around the standard 19-inch rack such as Rittal's TS IT and how the project operates with a similar ethos to OCP in that it rearranges server hardware to enhance airflow through the components. *www.rittal.co.uk*

■ Axios Systems is hosting a webinar that discusses whether organisations are using ITSM tools that are fit-for-purpose and helping them achieve their IT strategic vision for the 2020s. In a special one hour webinar, Stephen Mann of ITSM.tools will discuss how an ITSM tool should help reduce Total Cost of Ownership and unnecessary spending given the current wave of change within the IT landscape. Mann will explore the key elements that have forced this change in the ITSM tool marketplace, and what you need to consider when assessing your current tool and why you may need to change it. The webinar takes place at 4pm on 7 November. Register at *https://tinyurl.com/ya64m2xf*