APRIL 2021
networkingplus.co.uk

NETWORKING+

Autonomous cloud security

How firms can better optimise their cloud environment

Scott Dodds, Ultima, *p7*

The critical comms column

How would you define critical communications?

Mladen Vratonjic, TCCA, *p13*

Questions & answers...

A chat with the director of sales and engineering at Netskope

Andy Aplin, Netskope, *p16*

Government introduces legislation for smart devices

The UK government has announced plans to create new legislation that requires smart devices to meet new requirements to protect businesses from cyberattacks.

A planned new law to address the shortfall in device security will force suppliers to tell users at the point of sale for how long their product will receive security software updates and patches.

The Department for Digital, Culture, Media and Sport (DCMS) said it would now also be putting smartphones in scope of the planned legislation and said research had shown up to a third of users (businesses and consumers) keep their smartphones for at least four years, but many brands only offer security updates for two years.

Recent University College London research found that out of 270 products tested, none displayed this information at point of sale or in any accompanying paperwork.

"Our phones and smart devices can be a gold mine for hackers looking to steal data, yet a great number still run older software with holes in their security systems," said digital infrastructure minister Matt Warman.

Brad Ree, chief technology officer of the Internet of Secure Things (IoXT) Alliance, said "we applaud the UK government for taking this critical step" to demand more from IoT device manufacturers and to better protect the businesses that use them.

"Requiring unique passwords, operating a vulnerability disclosure programme, and informing consumers on the length of time products will be supported is a minimum that any manufacturer should provide," he added. "These are all included in the IoXT compliance programme and have been well received by manufacturers around the world."

NCSC (National Cyber Security Centre) technical director Ian Levy added that end-users have become "increasingly reliant" on connected products in the workplace. "The Covid-19 pandemic has only accelerated this trend and while manufacturers of these devices are improving security practices gradually, it is not yet good enough," he said.

The law, which will be introduced "as soon as parliamentary time allows" builds on a series of steps Westminster has already taken, including the publication of a code of practice for device-makers and the development of an international standard for IoT security, which has been approved by industry association the Cybersecurity Tech Accord.

Rick Jones, chief executive officer and co-founder at DigitalXRAID, said news that the UK government plans to protect the consumer from security breaches and data thefts with new requirements for technology manufacturers comes at a critical time for businesses.

continued on page 2

IN DEPTH: Network monitoring in a hybrid world
P8-9

Government introduces new legislation

Continued from page 1

"As many continue to work from home, using personal and un-secured devices to access company servers, network vulnerabilities have expanded dramatically," he said. "Smart devices in particular have evolved into extremely powerful PCs that can act as touchpoints for internal networks, yet they will have far less security than typical enterprise IT applications."

Jones added that as the Internet of Things (IoT) grows, smart devices are further integrated within expansive networks, opening up higher vulnerability to hacking and increased difficulty protecting sensitive data. "What's more, as one of many devices connected to IoT, a personal smart phone may be used to circumvent security, with hackers pivoting into the corporate environment," he said.

Jamie Brown, director of senior global government affairs at Tenable, said that it was time for manufacturers to be held accountable and not to put the onus on enterprises.

"To date, much of the responsibility for securing IoT products has been forced onto end-users by vendors," he added. "Subsequently, users are tasked with securing their own devices whilst often being unaware of the risks they are bringing into their offices. The ability to easily report discovered software bugs (vulnerabilities) is another element of this legislation that is to be applauded. This is the easiest way for vendors to be made aware of security issues within products, and take action, before they can be used nefariously." ■

'DC cooling infrastructure must be compliant ahead of summer'

Data centre operators must ensure cooling infrastructure being repaired or replaced is compliant with regulations if extreme heat reaches similar heights to last year, according to a temperature control specialist.

Affecting both the UK and EU, the 2020 F-Gas ban is a requirement of EU Regulation 517/2014 and means no refrigerants with a high global warming potential (GWP) can be used in cooling systems. For European data centres with mechanical cooling systems, this means refurbishment or replacement of aging infrastructure must be compliant with these regulations.

As Covid-19 may have disrupted maintenance schedules for data centres across Europe, it is imperative that cooling systems are compliant with regulations when being repaired or replaced. Continuing supply chain issues may mean that this process could be prolonged while waiting for equipment to arrive, if mechanical cooling is used.

Though many data centres may opt for a free cooling approach, rising temperatures across Europe caused by climate change may mean permanent cooling infrastructure reaches its limit. With this in mind, Nick Osborne, data centre specialist at Aggreko, is warning operators to plan for temporary cooling ahead of summer heatwaves.

"The Met Office has predicted we will see even more instances of heatwaves across Europe this summer, so data centre cooling systems are at risk of reaching their limit," Osborne. "If cooling demand exceeds capacity or the cooling system is awaiting repair or replacement within regulation parameters, unexpected and costly downtime is likely to ensue during critical periods. Data centre operators must ensure their plans for supplementary cooling for these heatwaves are in place now before the summer begins."

As Covid-19 may have disrupted maintenance schedules for data centres across Europe, it is imperative that cooling systems are compliant with regulations when being repaired or replaced

Given that the periods of extreme heat are limited, European operators may find it more practical to hire temporary cooling solutions to boost cooling capacity for the times. On top of ensuring F-gas ban compliance, outsourcing the supplementary cooling to a temperature control expert means the correct level of equipment can be selected and integrated easily into the existing infrastructure after site audits.

"With supply chain issues and financial uncertainty being key challenges of the past year, temporary cooling equipment hire could mitigate downtime while permanent infrastructure upgrades are made or free cooling methods are introduced," Osborne added. " We are more reliant on data centres than ever, so avoiding cooling failure-related downtime through careful planning is paramount to navigating the summer months." ■

University of Hertfordshire suffers major cyberattack

The University of Hertfordshire was hit by a cyber-attack that has taken down its entire IT network as well as blocking access to its cloud-based services. It revealed the attack occurred late on April 14 in a statement posted on its website. As a result, all its online classes scheduled today for the following day were cancelled.

The statement read: "Shortly before 22:00 last night, the University experienced a cyber-attack which has impacted all of our systems, including those in the cloud such as Canvas, MS Teams and Zoom. Please be reassured that our IT colleagues are working hard to rectify the situation as soon as possible.

"However, as a result, all online teaching will be cancelled today (Thursday 15 April), and we understand that this may impact students being able to submit assignments. We want to reassure our students that no-one will be disadvantaged as a consequence of this.

"Any in-person, on-campus teaching may still continue today, if computer access is not required, but students will have no onsite or remote access to computer facilities in the LRC's, labs or the university Wi-Fi. "We apologise for the inconvenience this situation has caused and will continue to keep you updated. You can check the status of all our systems by visiting https://status.herts.ac.uk/."

Currently, there are no further details about the nature of the attack, although there has been a sharp rise in ransomware attacks targeting higher education institutions in the last year. This partly as a result of additional vulnerabilities brought about by the shift to online learning during Covid-19. Last year in the UK, Newcastle and Northumbria Universities experienced ransomware incidents, causing significant disruption. ■

A statement read: "Shortly before 22:00 last night, the University experienced a cyber-attack which has impacted all of our systems, including those in the cloud such as Canvas, MS Teams and Zoom

Vipre releases latest cybersecurity defence bundles

Vipre UK & Ireland has released its latest cybersecurity defence bundles, providing businesses with protection at their core, edge or across the entire business network.

The latest packages marry the essential security foundations of e-mail and endpoint protection with the emerging necessities of security awareness training, web access control, protection from misaddressed e-mails, multi-layered DLP and cloud-based VPN.

"The cybersecurity landscape continues to evolve, and as the ongoing pandemic presents even more opportunities for hackers to strike, businesses need to implement the right solutions to strengthen their cyber defence strategy," said Andrea Babbs, UK general manager, Vipre Security. "A cyber aware culture with the right technology is crucial, and we aim to support organisations with a more comprehensive, multi-layered approach to security. With over 25 years of security expertise and one of the industry's longest-standing and experienced vendors, we want to help our customers on this journey to gain more from their security solutions. These elements cannot be considered in isolation, but instead as part of a journey for additional protection."

Vipre's security suites are available at three levels: core defence, edge defence and complete defence.

The former helps to protect the heart of a business' network. This includes endpoint security with the added benefit of web access control and business cloud VPN, securing organisations' networks, while reducing device and employee downtime if servers and workstations are targeted by ransomware and phishing attacks. The edge defence bundle protects the boundary of the organisation at the edge of the network, where employees use email to communicate with the outside world. The offering also includes additional elements, such as advanced threat protection and SafeSend DLP, aiming to build a smarter, safer workforce kept safe from misaddressed email and data loss.

The latter s bundle protects an organisation's entire network of devices, email, people and data, by not only encrypting, scanning, and validating email contents and recipients, but also enforcing acceptable use policies to reduce complaints and legal threats. This security suite of solutions brings all the advanced security solutions together, forming a 360 defence strategy. ■

EDITORIAL:
Editor: Robert Shepherd
roberts@kadiumpublishing.com
Designer: Sean McNamara
seanm@kadiumpublishing.com
Contributors: Gerry Moynihan, Darren Fields, Scott Dodds, Alex MacPherson, Mladen Vratonjic, Alex Thompson, Andy Aplin

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, Image Court, IC113, 328/334
Molesey Road, Hersham, Surrey, KT12 3LT
Tel: +44 (0) 1932 886 537

ISSN: 2052–7373

UBD appoints CDW as tech partner for new campus

The University of Birmingham Dubai has appointed IT services and solutions provider CDW to help create a high-quality technology environment for students and staff at its new campus.

Following a successful tender process, the company will provide equipment and support across the state-of-the-art campus. Students and staff will be provided with Lenovo laptops and the campus network will support WiFi6. Smart sensors across teaching spaces will map people flows - allowing the most efficient use of the buildings. Students will be able to structure their time on campus through dedicated mobile apps and smart scheduling.

These technologies will combine to provide students and faculty with a seamless suite of tools built bespoke for the University experience. The infrastructure is also modular by design to allow for future innovation and growth.

"Our new building has been designed as an 'Intelligent Campus' - embedded with flexible, cutting-edge technology allowing innovative, multidisciplinary teaching and learning," said University of Birmingham Dubai Provost, professor David Sadler. "CDW will help us to deliver a flexible and powerful teaching environment in Dubai that students and staff will enjoy. Everyone – students and staff alike – is eagerly looking forward to moving into our brand-new, bespoke campus building later this year. We believe that, in our new academic home, we will deliver an educational experience like no other in Dubai."

A university procurement selection panel, led by category manager (ICT) Thomas Hasson, made a recommendation to senior leaders who approved the contract award to CDW.

The company will oversee the full suite of technology solutions for the campus and the company is working with a number of strategic partners in key areas. Dell Technologies will take care of data centre computing and storage, Lenovo will provide devices, workstations and laptops, while Fortinet has been selected for firewall security. Meanwhile, Cisco will run WAN and LAN – including a true software-defined network, Rubrik will supply data backup, security and APC for power protection, while Infoblox is in charge of DNS. The Dubai campus is due to open Autumn 2021. ■

Following a successful tender process, the company will provide equipment and support across the state-of-the-art campus. Students and staff will be provided with Lenovo laptops and the campus network will support WiFi6. Smart sensors across teaching spaces will map people flows - allowing the most efficient use of the buildings

Harrow Council moves to the cloud

Harrow London Borough Council has deployed a cloud contact centre and communications product from 8x8 as part of its digital transformation agenda to enhance delivery of essential services.

The authority said it faced challenges that were common among UK public sector organisations, such as being hampered by legacy on-premises systems that were unreliable, costly to maintain and offering limited functionality.

These technology shortcomings were further exacerbated when the council's mission-critical "Access Harrow" contact centre and telephony system struggled to support employees and contact centre agents transitioning to remote work.

Harrow selected 8x8's integrated cloud contact centre and communications platform to replace its legacy systems with a view to improving manageability and reliability, ensuring business resiliency, enabling an operate-from-anywhere workforce, and reducing costs.

"As we made a smooth transition into the cloud, the 8x8 delivery team was with us every step of the way, ensuring we were ready to make the switch. The level of support they provided those initial weeks made what felt like a mammoth task more manageable," said Ben Goward, ICT director at Harrow Council. "Working with 8x8 has enabled us to adopt a nimble, hybrid approach, allowing our staff to work from anywhere while providing residents, businesses and visitors with the essential services they require."

Working with 8x8, the council equipped its 160 Access Harrow operators with the ability to engage customers across voice and digital channels while having a 360-degree view of customer needs and interactions. The result was a streamlined employee and customer experience with advanced analytics and reporting, allowing operators to consult and collaborate with colleagues to resolve customer issues through immediate access to relevant information, 8x8 reports.

More than one third of London's Borough Councils now use 8x8's services, it said. ■

FROM THE COVER

Getting to grips with NIST means better cyber security

The National Institute of Standards & Technology's (NIST) cybersecurity framework is often seen as a global standard for keeping businesses safe from cyber threats, but with the huge amount of useful information, it's easy to get lost in the detail. This summary will help get you started.

Identify and detect

The 'identify' and 'detect' elements of the NIST framework advise organisations to develop and implement effective ways to detect a cyber breach. This can take many forms, but scanning for breaches, anomalous behaviour and constantly checking data are important. If conducted manually by internal staff, this is time consuming, but automation can go a long way to lighten the load.

Powered by the latest AI and machine learning, a Security Information & Event Management (SIEM) platform can automate many processes and free up staff to investigate more serious events that require manual intervention. If you fall victim to a cyberattack, knowing about it quickly is essential in minimising the damage.

Protect

The 'protect' element of the NIST framework primarily cover prevention in the core areas of network, cloud and endpoint. The network perimeter is becoming ever more virtual, but that doesn't mean it's not important to protect with firewall, SD-WAN and DDoS protection solutions. Whether using public, private or hybrid cloud, clear lines of responsibility for data security and policy enforcement are critical. And finally, the endpoint or user is the most common breach vector so keeping users safe browsing the web, opening emails and downloading files is a key task.

Prevention also covers processes and people; according to a report created by the UK government, 48% of businesses have a basic cybersecurity skills gap. Consider outside help in the form of management service options, or a virtual Security Manager to act as an extension to your IT team.

The NIST framework advocates comprehensive awareness and training for all staff. Having systems in place to prevent a hacker accessing your network is no good if staff fall foul of a phishing e-mail with the same result.

Respond and recover

The 'respond' and 'recover' elements include response planning, mitigation and recovery activities to ensure continuous improvement. Start with an incident response plan covering key dependencies, backup and recovery solutions and any legal or regulatory requirements, to minimise damage and ensure you don't leave systems open to further attack.

A cyber breach can cause prolonged downtime - being able to restore systems quickly is essential to keep your business running and your customers happy. NIST can be an intimidating framework but focus on these core areas to get you started and move on from there and you will significantly strengthen your security posture.

By Steve Burden, Head of Security, Daisy Corporate Services, dcs.tech

Arup staff hit by cyberhacker

Engineering and architecture giant Arup has been hit by a ransomware cyberattack, the company said. Hackers used ransomware to hit the global consultancy's third-party payroll provider, copying and encrypting files before demanding money for their release. Arup employs more than 6,000 people in its 16 offices across the UK, including around 40 architects. According to data breach specialist CEL Solicitors, Arup employees had their personal details, including bank details, address and name, compromised following the attack. It says it has already received enquiries from some staff members seeking advice on the data breach. Arup alerted its employees to the incident in a letter stating that the payroll provider Symatrix had suffered a 'cybersecurity incident' January 12.

GTT supports SGN's cloud transformation

GTT Communications has signed a major cloud deal with SGN, owner of one of the UK's largest gas distribution networks. Under the terms of the deal, GTT will provide cloud networking services, WAN and LAN services, DDoS mitigation and will increase the scope of professional services delivered in support of its cloud transformation strategy. "We value our strategic partnership with SGN and look forward to continuing to support its next phase of IT transformation with our secure cloud networking and professional services capability," said Tom Homer the president of GTT's European division.

Six Degrees has management re-shuffle

Secure cloud services provider Six Degrees has made management changes to further strengthen the company's growth ambitions. Effective from 1st May 2021, current CEO, David Howson, will become chairperson of the board and Simon Crawley-Trice, currently practice group managing director, will assume the role of CEO. Howson's transition to chair comes after four years as CEO Prior to joining Six Degrees in October 2020, Crawley-Trice was on the EMEA executive team at Rackspace where he led its growth in public cloud, application, data managed services and professional services propositions across EMEA and the USA.

Coventry businesses get big fibre boost

Thousands more businesses across Coventry will be able to access full fibre connectivity now CityFibre has extended its build in the city. The company is adding a further £12.5m to boost its original £60m investment in Coventry, which has already brought the best available connectivity within reach of tens of thousands of premises across the city. Last month, CityFibre hit a major milestone in Coventry when it officially passed the halfway mark on its original build plan. Work is now currently underway in a number of locations across the city including Tile Hill, Allesley Village, Binley and Walsgrave. "We're making huge strides in delivering full fibre to homes and businesses across Coventry, and we're thrilled to now be bringing our best-in-class network to communities in the west of the city," said Leigh Hunt, CityFibre's regional partnership director and city manager for Coventry.

MPLS usage drops as SD-WAN adoption ramps up

The migration from networks based on multi-protocol label switching (MPLS) to the more agile and affordable alternative, software-defined wide-area networking (SD-WAN), continues apace, according to the latest WAN Manager Survey from global telecommunications market research and consulting firm TeleGeography. "Our annual WAN Manager Survey always provides interesting insights into enterprise networking trends globally, but has been of particular interest this year due to the impact of the pandemic on our findings," said Greg Bryan, senior manager of enterprise research at TeleGeography, The report aimed to offer a clear picture of how mid-size to large enterprises are adjusting to emerging WAN technologies, helping suppliers make more informed decisions.

Secure I.T. Environments extends University of Chichester contract

Secure I.T. Environments, the design and build company for modular, containerised and micro data centres, has extended its long-standing relationship with University of Chichester. The new multi-year maintenance and support contract will see the work across the university's two sites at Bishop Otter and Bognor. It covers a range of services including repairs, support and preventative maintenance and room cleans at both sites. Secure I.T. Environments will be responsible for all room infrastructure including air conditioning, fire suppression, UPS systems and generators. "We're very pleased to be extending our relationship with University of Chichester, which we have worked with at different times for over a decade,

including previously building a new data centre," said Chris Wellfair, projects director at Secure I.T. Environments. "The institution shares our commitment to high standards of support and maintenance in the data centre industry."

TeamViewer adds additional security

TeamViewer, the provider of secure remote connectivity solutions and workplace, is adding an additional layer of security to its products with the launch of Two-Factor authentication (TFA). This security upgrade is in line with its ongoing commitment to provide the most secure remote connectivity solutions to their customers. TeamViewer accounts can be secured with two-factor authentication already, which is recommended by security experts. From now on, incoming connections can be secured with TFA in addition to raising awareness of every connection established at any point in time. The optional security feature can be set up for all TeamViewer remote control connections and is executed via push notifications.

PCTEL joins TCCA

PCTEL, the global provider of wireless technology including purpose-built antennas and test and measurement solutions for public safety communications, has become a member of TCCA, the global representative organisation for the critical communications sector. A global company headquartered in the United States, PCTEL designs and manufactures antennas and test and measurement solutions for critical communications applications. Public safety fleets worldwide use PCTEL antennas for high performance P25, TETRA, DMR, FirstNet/LTE, and 5G connectivity. First responders depend on these networks for in-building communications.

Word on the web...

Device management solutions can help your business, by Nadav Avni, Radix Technologies

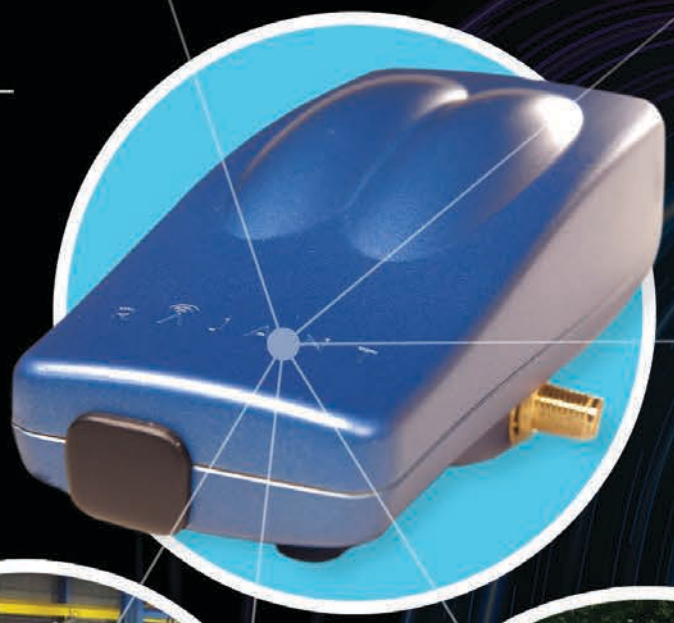
To read this and other opinions from industry luminaries, visit www.networkingplus.co.uk

Just like today's industrial leaders, Rajant's network is

Smart. Autonomous. Always moving.

Rajant Kinetic Mesh® is the only wireless network to power the non-stop performance of next-gen applications—from real-time monitoring to robotics and AI.

- Works peer-to-peer to maintain **hundreds of connections simultaneously for 'never break' mobility**
- Intelligently self-optimizes to **change in real-time, ensuring mission-critical reliability**
- The *only* network to enable **machine-to-machine communications required for autonomy**
- Provides **Industrial Wi-Fi for extended Wi-Fi connections** in challenging environments



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

*Industrial Wireless Networks **Unleashed.***

Download our **"Why Carrier-based LTE and Private LTE Just Aren't Enough for IIoT"** white paper at **rajant.com/networkingplus**

RAJANT

Zero-trust networking

A safe journey to a better employee experience, by Darren Fields at Citrix

Imagine you are in a foreign city for the first time and need to take a taxi cab to reach your destination. When hailing a taxi, the only thing you can go by is a quick inspection: if it looks like a taxi, carries the typical "taxi" sign, a taxi registration number, and the name of a taxi company written on its doors, you get onboard – unless the car, again at first glance, is in terrible shape.

As soon as you have taken your seat in the cab, you need to trust the driver: you need to assume that they will take you to your destination smoothly, won't endanger your safety by speeding or drunk driving, and will avoid unnecessary detours. This is always a somewhat uneasy feeling – but we cope with it.

From the bird's eye view of an IT team tasked with securing the company network, all user accounts look like little taxi cabs: the "vehicles" employees use to navigate the company's data highways are their endpoint devices, their "taxi license" is their user profile and the associated access password – and, just like real-world taxi cabs, they can have accidents or even be hijacked by threat actors. So, while companies used to be content with an initial showing of papers, today's IT and network security teams cannot simply assume that these taxis will drive safely and responsibly – they have to make sure.

There are two main drivers (no pun intended) for this change: first, in today's business world, practically all business processes depend on a reliable, secure

IT infrastructure. So the IT security team is required to have a close look at who way is using this infrastructure in what way. Second, today's user base is far more heterogeneous than it used to be. While twenty – or even only ten – years ago, most users would probably access company resources by using company devices from within the company network, the current situation is vastly different – and much more complex.

Even before the current crisis with its lockdowns and the boom in home-office and remote work scenarios, employees used to work ever more flexibly: they increasingly accessed apps and data from anywhere – from home, from a hotel on business travels, from a train or plane, or from their favourite café. They had long started the "bring your own device" (BYOD) trend of using privately-owned devices instead of just company equipment. Also, more and more of the apps and data they accessed would not reside only in the company data centre anymore, but in the cloud – usually in a variety of public clouds. Today's digital work is shaped by increasing mobility and flexibility, and recent Citrix surveys suggest that even after the current crisis, this trend towards more flexible remote work will continue.

So the challenge is to guarantee the required level of security in an increasingly complex environment. To achieve this, the zero-trust approach replaces the initial "at a glance" security control, instead following the rule, "never trust, always verify": in a ZTNA, security software based on AI algorithms continuously monitors user (more specifically: user account) and endpoint device behaviour, checking for deviations from defined rules and historical behaviour patterns.

Darren Fields, regional vice president, cloud networking, EMEA at Citrix

For this, the first step is to continually verify the user's identity, ideally by applying multi-factor authentication via hardware tokens or soft-token apps. The second step is endpoint device monitoring, from the devices' ownership status (company-owned, privately owned) to their patch level. This non-stop vigilance allows the ZTNA infrastructure to immediately react to suspicious activities, for example if a log-in request comes from London, but one minute later the next request comes from, say, Singapore – a clear sign of a user account takeover. In this case, the ZTNA software can alert the security team or even, if permitted to do so, automatically block user access. In other cases which are not quite as clear, the software might ask users to provide additional proof of their identity, e.g. by using a second authentication factor. For information security, users' access to resources can be limited to what they actually need to access in their respective roles. This is complemented by customisable rules that restrict user access based on their current context: user X may be allowed access any kind of apps or data from anywhere with any device, but user Y may only use e-mail and the web remotely, while user Z may only access sensitive business intelligence data using two-factor authentication and a corporate device.

It is important to note that when implementing ZTNA, the focus needs to be on the employee experience: access policies should be designed to give the users all the flexibility they need in their usual business day. Once this set of policies is established, the beauty of ZTNA is that the software will use AI to automatically determine a baseline of regular behaviour, and will only intervene if there is a reason to be suspicious. This means that most of the time, users won't notice the AI algorithms working in the background at all. This makes zero-trust networking much more employee-friendly than traditional IT security solutions: ZTNA strikes a perfect balance between resilient security and hassle-free usability, so employees can work without distractions or interruptions, but with the comforting knowledge that their digital workspace is secure.

In other words, a zero-trust network architecture – either as an integrated component of a digital workspace environment or as a stand-alone ZTNA solution – will always have a close eye on the taxi driver – not only upon entering the cab, but throughout the whole trip. This way, ZTNA gives employees a safe journey through today's complex hybrid multi-cloud world. Zero-trust – in spite of its name – continuously establishes the trust needed for an efficient, secure work environment with a great employee experience. ■

Autonomous cloud security

Scott Dodds, CEO, Ultima

The Covid-19 pandemic has created exponential growth in companies requiring cloud services, but their IT staff don't have all the technical skills to effectively and safely move them to the cloud. This leaves companies open to security vulnerabilities as well as meaning they are not optimising their cloud environment.

While many businesses have risen to the challenges of remote working, infrastructure and security remain an issue. But automated cloud services with in-built security solutions can solve these problems. They can be bought on a pay-as-you-go basis, addressing large CAPEX outlay issues and allowing companies to overcome legacy application issues and provide security that protects both employee and company from outside attack.

For those companies who've still not made the leap to the cloud, automated cloud migration services exist that can overcome the financial and skills shortage barriers to entry. Managed Service Partners (MSPs) can provide technical expertise and technical solutions to make this possible. The results of moving to the cloud can be spectacular too: from an average 30% reduction in expenditure and up to a 750% increase in productivity. They also have no upfront costs.

Using Microsoft Azure's open and flexible cloud computing platform, for example, combined with automated migration, you no longer need to look after and buy hardware, or sort out power and cooling. Your IT infrastructure and security can be run on a pay-as-you-go basis. And if you need increased capacity, automation means you can extend your on-premises data centres and infrastructure to Azure within a few hours, providing the extra capacity required for critical systems and applications.

We know that traditional security solutions don't work well in the cloud. When customers move to the cloud, they try and take their traditional security solutions with them. But as the cloud works in a very different way to on-premises, this leaves companies open to vulnerabilities. You need a made for purpose solution, based on cloud security best practice.

With the latest automation technology security and monitoring solutions are automatically applied to existing and new workloads. It scans the collected data and includes proactive monitoring around security events that will let you know exactly what's happened in clear-to-understand alerts, and where action should be taken if needed, covering critical areas such as anti-malware. IT staff can view in real-time their security and compliance reporting. Soon we will be able to scan a customer's environment for security-related bad practice or incidents and make recommendations on how to fix them and even give them a score as to how they are doing.

At Ultima, we've also found that on moving to the cloud customers have poor visibility of what is going on in their environment. We know about 25% of companies don't even realise they have high severity patches missing. This is down to a skills shortage and a lack of time – as patches are often done manually.

With automated cloud services, patching happens automatically on repeat and even scales as your infrastructure grows. If a patch is due and fails for whatever reason the system will automatically create an alert. This information will go to the third line technical team, and they will investigate it themselves, whether that's your MSP or your own IT staff. The time savings to the IT department are huge – often 100s of hours a year - enabling them to focus on other projects and have peace of mind about security.

Traditionally, you would do a true-up every month or quarter of your IT environments to bring new things, including security issues, to the management. But when you are in the cloud, you can spin things up so fast, that you will have a gap if you are only doing a true-up every month or quarter. With an automated service, you can automatically onboard things, so you don't have to wait for the true-up process, which means you have a more proactive security service and less vulnerability. We've found that customers who are using automated cloud services have a 66% reduction in security incidents.

With ever increasing cloud resources, it can be hard to get visibility into your cloud infrastructure. The technology exists now to automatically scan and configure your cloud resources with centralised logging and telemetry capabilities. As your environment grows, this process repeats itself automatically as it scans and configures itself when new resources are added. This means that all logging information is available, and you can also see on one dashboard insights into your security posture. Usually, it's hard to see what's happening from a security perspective – what data is coming in and going out, top destinations, any malicious activity detected in the last 24 hours, etc. Automated services give customers a dashboard that centralises all the information to see what is happening in a simplified format and how your infrastructure is performing at a high level.

These new autonomous cloud services enable companies to free up 100s of hours of IT staff time and reduce security incidents. Moving to the cloud has previously been a struggle for some companies as costs escalated for support, maintenance and security. New technology has changed that and is ensuring security and infrastructure are no longer barriers to successful cloud deployments and productive, flexible working.

Network monitoring in a hybrid world

Businesses rely on their WAN and LAN to perform at levels high enough to satisfy their clients' demands. But how will that work in a hybrid world? Robert Shepherd investigates

In 2021, we face more network vulnerabilities, security attacks and data breaches than ever before in the history of IT and communications. This has increased the demand for stronger network performance and the tools used to manage the network. Given this, it's imperative businesses find a way to accommodate all of these systems and networks with the right network monitoring and security tools to protect our corporate assets and - of course - the bottom line.

Neil Collier, co-founder and technical director of GCH Test & Computer Services explains how using the internet for all users has changed significantly since March 2020 when the Covid-19 pandemic spread across the globe.

"Millions of people in most market sectors were used to working centrally but have been relegated to working from home," he says. "One of the consequences of this shift was that instead of internet traffic primarily being LAN-based, concentrated in the data centre, connections became WAN-based. This shift brought new challenges; laptops and desktop computers in homes replaced the in-house LAN environment. Every home worker became dependent on broadband and network administrators had to handle increasing calls from staff who may not know how to fix connection problems."

It's also important to know that it isn't an Orwellian approach monitoring, so before you scramble to delete your internet search history, it's not "that" kind of monitoring, according to Mathias Hein, consultant at Allegro Packets.

"Network monitoring may sound like 'Big Brother is watching you'," he says. "In fact, it is not like this at all. Networks are complex - the internet, a massive number of interconnected networks is even more so; efficient tools are needed to ensure they function as designed, so problems can be detected and fixed as quickly as possible."

Hein adds that monitoring does not interfere with the flow of data across networks and that it displays and often stores some or all voice, video and other data traffic generated by devices. "It is relatively easy to locate network faults that, for example, may drop a connection for a long period," Hein continues. "It is more challenging when faults occur sporadically and in short time spans. That is when efficient, easy-to-read network monitoring equipment is a vital asset to an organisation. It is even more valuable if the monitoring device can store back-in-time data, particularly when searching for a transient problem."

Time now, then, to take a look at how things have changed in the past year. After all, most UK office workers were forced to connect to the company network from home. Did that mean network monitoring had to evolve at short notice?

Adrian Rowley, senior director EMEA, Gigamon says the dramatic shift to remote working caused networks to turn inside out and become significantly more complex. "Unsurprisingly, with the increase in personal and unsecured devices connecting to a company intranet from around the world, visibility has been clouded and network vulnerabilities have been exacerbated," he says. "In fact, according to a recent survey, businesses cite remote worker endpoints as their biggest current security risk. With this move to remote working, traffic paths have changed and organisations need to ensure their existing tools are still working effectively and efficiently with the new traffic flows in their infrastructure."

"With the vast majority of employees working from home, IT teams had to change the way they monitored network traffic," says Chris Bihary, CEO and co-founder of Garland Technology. "Did employees still have access to all of their resources on cloud-based applications, or were they using a VPN to access the corporate resources behind a firewall? Software defined perimeter technology became prevalent with users only having access to authorised applications to help reduce threats from compromised devices."

Chris Labac, vice president, global sales engineering, Viavi Solutions adds that in today's remote working world, where many IT departments are limited to remote access to users and their endpoints, the need for comprehensive infrastructure monitoring and insights into the remote end-user has never been greater. "An integral part of this is the ability to flexibly instrument and maintain service health where users are located or applications are hosted," adds Labac. "The State of the Network 2020 uncovered that last year, during the start of the remote working crisis, the surge in remote users challenged 58% of IT professionals to seek more network visibility in order to manage bandwidth load, monitor application performance and avoid VPN oversubscription."

"With the vast majority of employees working from home, IT teams had to change the way they monitored network traffic"

Chris Bihary, CEO and co-founder, Garland Technology

Labac added that this year, "we are seeing an increased investment in IT technology", with more than 70% adoption of emerging technologies such as SASE, SD-WAN, 5G, and IoT. "In the post-remote workforce world, the need to have visibility into these now mainstream technologies and ensure that the end-user's experience is maintained before and after deployment has become critical," he says.

Now that the UK has a so-called 'clear roadmap' to cautiously ease lockdown, many, if not most of the British workforce will see a 'new normal' in the form of hybrid working. With that in mind, Chris Bihary, CEO and co-founder of Garland Technology, opines that 'SASE is here to stay' as it gives IT teams greater flexibility to deal with changing needs of remote workers. "Using SASE administrators combine security technologies such as Zero Trust Network Access and Firewall as a Service (FWaaS) with network technologies such as SD-WAN," he says. "This produces a flexible network that can create secure connections between users, defended by a security implementation that's both lightweight and powerful. Under SASE, security is consumed as a service and partly managed by vendors. Because users no longer need to route their connectivity through the data centre to access their tools, they can gain an advantage in terms of reduced latency and thus increased productivity."

Hodgson says that Paessler doesn't "see a fundamental change for network monitoring" due to hybrid working. "Nothing completely new happened but the focus has changed. Cloud applications, collaboration tools, and video conferencing have become vital parts for many companies and will not vanish once the pandemic becomes a thing of the past," he continues. "But, also on premises will remain part of our daily business. Performance and security reasons make it indispensable for the foreseeable future. Network monitoring will need to improve when it's about monitoring cloud applications and services, but this still needs all the on-premises features."

Then, of course, there's technology. To successfully carry out network monitoring, key technology is required. Rowley says "the hero technology of the past year has been cloud", which he says has been the bedrock for remote workers separated from their teams.

"However, many businesses did not have the time or resources to implement the correct infrastructure needed for the rapid digital transformation initiatives required by the pandemic and were instead forced to upgrade their solutions in a patchwork fashion," he continues. "For these organisations, migration to the cloud was rushed, yet it continues to play a critical part in business agility. The issue now lies in the fact that legacy network monitoring systems struggle to cope with a hybrid cloud model."

Rowley adds that "it's impossible to sufficiently monitor the cloud with tools made for on-premise systems, while cloud tools themselves can often rely on application-level telemetry, and therefore lack visibility into the critical data moving across the network". He continues: "For network monitoring in this new environment, NetOps teams must find visibility solutions that span the entirety of the hybrid cloud, thus eliminating blind spots and reducing security risks. Ultimately, the key technology here is a platform which allows complete visibility from the core to the cloud."

It's a view shared by Labac, who says the latest network monitoring tools implement automation and machine learning (ML) to automatically flag root cause of problems, making it easier for staff to address them.

"For example, the Viavi Observer platform uses automated workflows to provide an end-user experience score – a patent-pending technology that leverages ML to combine more than 30 key performance indicators (KPIs) into a single score that includes problem domain isolation," he adds.

Even with all the right kit in place, problems can still occur – so what can be done about outages, alert fatigue and excess tools? Hein explains that "outages can be disastrous," and that "we are all dependent on computers for our work life and outages", depending on the organisation affected, can create financial meltdown or be life-threatening.

"While security mechanisms and software are an essential component of networks, the same is true for monitoring solutions," Hein adds. "Powerful, easy-to-use and manage monitoring technology is not an option, it should be recognised as a mandatory component in a network. Alert fatigue can be the result of having to watch too many tasks at the same time due to insufficient or inadequate fault reporting tools and poor User Interface design. As for the tools themselves, well crafted, intuitive User Interface design can simplify the task of the administrator and help locate and fix problems in a timely and efficient manner."

Hodgson explains that many monitoring tools have a very in-depth approach to delivering deep analysis even if it's not necessary for avoiding failures. That, he explains, leads to many specialised tools, each of them with its own alerting functionality. "You could then use alert management tools to handle all those specialties, but you will have to pay to maintain all those single tools," Hodgson continues. "The other approach is to use one solution with a broader approach that can replace two, three or even more of those specialised tools and combine it with specialised tools for vital areas like advanced traffic analysis."

"It is relatively easy to locate network faults that, for example, may drop a connection for a long period"

Mathias Hein, consultant, Allegro Packets

Future-proofing is key for all businesses and that is also true when it comes to network monitoring. After all, in the modern era, no network means no business. That means companies will find it incumbent upon them to review their existing set-up.

"It may be time to re-evaluate your monitoring tools or platform when you are upgrading your network speeds, say from 1G to 10G or even 100G, if you regularly are experiencing network degradation, slowdowns, or lack of capacity," says Bihary.

"If you find it difficult to monitor all of the different areas of your network, both on prem in the data centre and in remote sites, and in the cloud. After you experience a breach or hack, you may want to look at the monitoring tools you have in place to see how you can mitigate the effects of that breach, and work to prevent future attacks."

For Hodgson, the "key indicator" for companies to re-evaluate is when they realise that the number of monitoring tools is constantly rising.

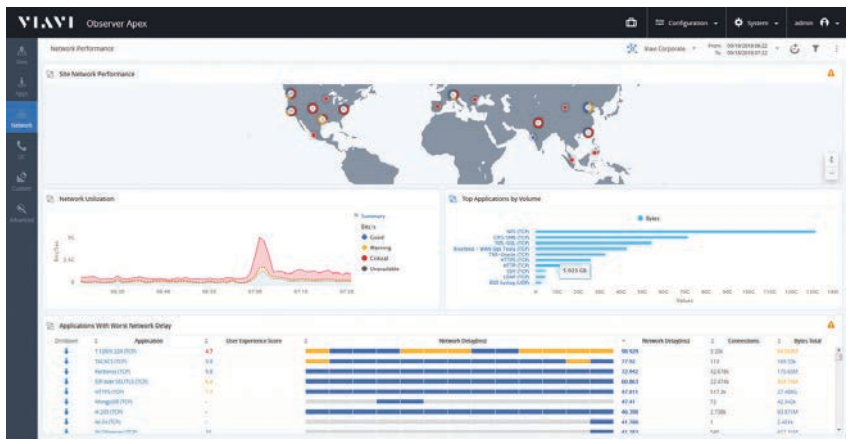
"Usually you don't replace an existing tool as long as it works, but more likely add another one for additional tasks," he adds. "Depending on the size of the company this can sum up to five, ten, or even more separate monitoring tools. At a certain point managing those tools will eventually take more and more effort, which should be the prompt for you to start thinking about replacing some of them with broader, more efficient tools."

As far as Labac is concerned, there are many signs that it may be time to re-evaluate a monitoring tool but the "canary in the coal mine" indicator will be declining customer and stakeholder satisfaction with poor IT user experience. "Others include frustrating interactions with services and support team. However, the most critical issue may simply be that the tool is not easy to implement," he continues. "As the skills gap is expanding and IT resources are already spread thin, ease of use and accessibility is the single most important indicator that you're using the right tool. If your team is finding themselves overwhelmed with KPI overload, or with an inability to easily drill down into forensic level data, then it's a clear sign that you may want to seek a different network monitoring platform."

The future of the network is far more complex than we could have imagined. The consumerisation of IT, mobile devices, big data, virtualization and cloud computing are just some examples of

today's rising trends. But these trends also bring their own new complexities and challenges for the average enterprise.

Rowley says that as IT budgets remain tight following the financial uncertainty of the previous year, many IT teams are also facing the challenge of doing more with less. "In order to ensure efficient network monitoring is possible, it is important to consider where legacy, on-premise tools can be optimised and where existing technology can be upgraded to improve visibility," he continues. "By leveraging visibility to minimise the traffic being shared with each network tool, they can be optimised and budgets are more likely to be signed off by an organisation's financial decision-makers, as a cheaper and less dramatic overhaul of current infrastructure is possible."



In today's remote working world, where many IT departments are limited to remote access to users and their endpoints, the need for comprehensive infrastructure monitoring and insights into the remote end-user has never been greater

Regardless of what we do for a living, we are all dependent on computers and networks and as Collier points out, even the smallest fault can become costly to locate and rectify. He argues that this task becomes more complex when, instead of a centralised topology, internet traffic is pushed to the edge, a paradigm shift from normal network configuration. "Not every home worker benefits from high-speed broadband or the latest computer/internal infrastructure, so increasing pressure is put on network administrators," he says. "Two important software applications have escalated as a result. virtual private networks (VPNs) have become standard for many to help improve end-to-end security, and VoIP coupled with online conferencing has come of age. However, along with these applications, end-user misunderstanding, mis-configuration and network complexity means powerful, easy to use, network analysis equipment is crucial."

Collier argues that while many have prophesied that the conventional workplace is history, "perhaps such statements may prove to be inaccurate." He continues: "People are social creatures and need to be together; online conferencing, useful as that is, it cannot take the place of real face-to-face gatherings. Even so, for some, home working and dependency on reliable data connectivity is here to stay, and so is the need for smart network monitoring and analysis technology."

What we do know is that a strong security posture is only possible when there's pervasive visibility across the entire network and this is why solutions vendors are focused on providing today's enterprises with advanced network monitoring and security solutions that provide intelligent visibility into the network in real-time.

Network outages and other problems can be very costly for businesses to address, not to mention very infuriating. To help enterprises operate as healthily as possible, networking monitoring has long been an invaluable service – as old as the networks themselves – in keeping businesses going in the face of adversity. It will also change with the times. ■

"One of the consequences of this shift was that instead of internet traffic primarily being LAN-based, concentrated in the data centre, connections became WAN-based"

Neil Collier,
co-founder and technical director,
GCH Test & Computer Services

Why retailers need to put their heads in the cloud

Alex MacPherson, director of solution consultancy and account management, Manhattan Associates

If theCovid-19 pandemic-induced disruption to retail in 2020 taught retailers anything at all, it's that the need to be flexible is crucial not only to business continuity, but to business survival. The seemingly never ending uncertainty caused by repeated lockdowns, social distancing, lack of clarity as to what you could and couldn't do, having to work from home with no end in sight - not to mention finally "getting Brexit done" – has had an enormous effect on society as a whole. Combine that with the closure of non-essential shops and the rise of ecommerce has had just as big an impact on retail as an industry too. .

It's clear there is a requirement for retailers to be agile, pragmatic and fleet-of-foot, and yet many retailers are still using rigid legacy systems that are already outdated at the point of installation and often lack the resilience needed to operate within the industry today.

Encourage innovation

Implementing a cloud-based system promotes business innovation and improves efficiency. Why? Well, with legacy on-premise solutions, organisations are stuck facing numerous time-consuming upgrades in order to get to the newest version of the technology. The only innovation coming into the business will be when the system gets upgraded and even then, companies will have to wait until the next upgrade - which could be years - in order to introduce the newest developments, meaning that companies miss out on improvements which benefit the entire organisation.

At this point, any chance of innovation is lost, leaving retailers behind the pace and a crowd of fed-up customers in their wake. Working in the cloud and with microservices specifically, however, enables retail organisations to continuously innovate, without the roadblocks of constant hardware upgrades, so that new ideas, systems and processes can be implemented rapidly to stay ahead of the curve. By freeing up internal IT capacity – which let's face it, comes at a premium in most organisations – working in the cloud means that more time can be spent on performing value-add services. Consequently, innovation will flourish, rather than just focusing attention on business-as-usual activities and maintaining vital systems.

Respond quickly to changes

If 2020 taught us anything, it's that the rate of change is even more rapid than we may have ever thought. Being able to adapt and respond to changes in an instant is now no longer a 'nice to have' competitive advantage, it's essential. Organisations that choose to move to the cloud will have the capacity and ability to respond to changing consumer demand and behaviour, rather than becoming stagnant and settled.

When shops shut their doors for the first time in March 2020, the retailers that were able to respond to these changes by adapting their Click and Collect networks, offering curbside pickup, turning their stores into mini distribution centres and collaborating with other local businesses were able to do so because their systems were flexible enough to handle the rapid changes.

Additionally, having the ability to quickly react to trends or seasonality changes; such as fashion retailers who could immediately offer loungewear on a larger scale, instead of office wear, when people were working from home, meant that less stock was being left to face large-scale discounts when stores were able to reopen. From Order Management Systems, to Warehouse Management Systems, retailers with a cloud-based approach were able to add new processes in a matter of hours, meeting customer demand - and customer expectations as a result.

Supporting business continuity

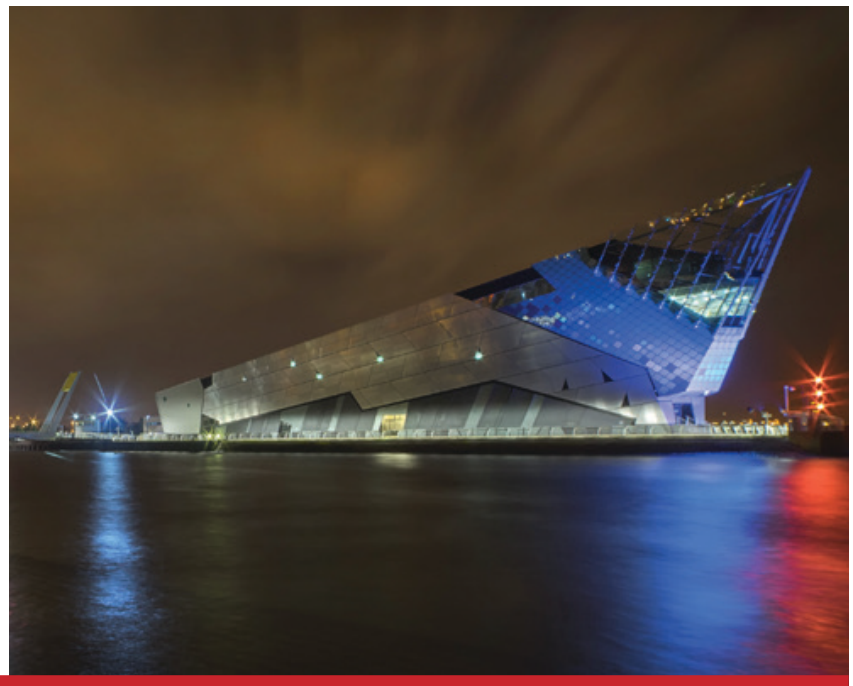
For manyif not most, the pandemic saw a halt to normal business practice and the realisation that a high-level of agility was needed in order to respond to industry developments at a supply chain level. Having a system that maintained business continuity was essential at a time when retailers frantically working like mad behind the scenes to maintain 'normal' levels of customer service.

Being able to upgrade seamlessly, without having to worry about every upgrade cycle or new IT deployment required enables this level of continuity and agility. At a time when so many other challenges and changes are being faced on a near-daily basis, being able to rely on this level of business continuity is something every retailer can take advantage of now and going forward.

Conclusion

The drastic changes in the retail industry alone since Covid-19 arrived on these shores in early 2020 have demonstrated how vitally important it is to have a level of flexibility, agility and pragmatism in order to adapt, evolve and survive. In our daily lives we don't care or even think about what version of an app we use on our smartphones - it doesn't matter - and this consumerisation has certainly filtered into enterprise thinking over the last few years too.

In an increasingly digital-first world that is constantly advancing, innovation and business continuity are two of the key pillars for all industries - no, not just the retail sector - and the best way to achieve these goals is to turn to the cloud.



Hull's plan to become one of UK's first smart cities

East Yorkshire council sets out ambitious plan to take advantage of the principles being applied by the international Open Government Partnership

The strategy will see the city use data and technology to change how different departments in the council operate, and how they work together to deliver services across Hull.

One area of focus is how the Street Team responsible for traffic planning and management, use data to make more informed decisions on how to manage traffic and people flows around the city, determine bus routes and cycle paths, but also work more closely with the authority's Planning Team.

For instance, in the past, planning decisions for new buildings have been based on models using a combination of data and hypotheses on aspects such as traffic flows and parking. While modelling has reached a high standard and can make sound predictions, it is still a model and not always a true reflection of what will happen.

The strategy recognised therefore that using real-time passenger traffic data on how, when and where people come into, move around and exit the city, would not only help the Street Team better shape the road network, parking facilities, and anticipate potential pressure points, but also avoid detrimental planning decisions.

Giving both teams the capability to interrogate the data would help them better understand and anticipate the impact of their decisions. For instance, the Street team would be able to spot pinch points and change the flow to keep people moving at rush hour or on match days, but also advise of areas that are a 'no-go' for the Planning Team.

Similarly, the Planning Team could refer to more accurate analysis when assessing a planning application and make a decision with confidence that any impact a development would have would be positive or could be managed. And in instances where this is not the case, they could provide guidance on how the planning application needs to be refined.

Working with Citi Logik, experts in the field of traffic management in smart cities, the council has developed a technology plan to make this vision a reality.

Over the coming years it will build a Smart City Platform, which will integrate all the data the city holds and make it accessible across departments and more widely to the public and other NGOs like universities for example. What's more it will use artificial intelligence to make highly accurate real-time predictions and assessments using data from across the city so the teams can better manage the challenges they face and make more strategic decisions.

One aspect of the strategy is to consider smarter traffic management. As such, the council has implemented Citi Logik's Citi Analytics application, a web-based tool that helps cities understand traffic congestion and people movement using internet of things data, such as mobile network information from Vodafone and other IoT data sources including real-time GPS data from vehicles, and cellular data from pedestrians.

The tool is capable of processing billions of data events a day so that journey times, and traffic volumes can be understood and better managed. For instance, traffic jams could be predicted 15 minutes before they happen, and traffic re-routed to avoid it materialising at all. Crucially, the data is depersonalised so it can be used by organisations without risk.

Citi Analytics also provides access to easy to build and use real-time dashboards, as well as reporting and accurate modelling. This has made the application quick to implement at Hull Council, with minimal disruption to staff, and fast to deliver results. Now traffic and planning teams can interrogate the data and get meaningful insight on a scale that's not been possible before.

The council's strategy also reflects a need to improve the management of air pollution so, a collaborative programme has been put in place to improve monitoring pollution levels, using funding from Innovate UK. The intention is to bring together experts from the council, and Future Cities Catapult, a government supported centre for the advancement of smart cities, with Citi Logik technology to calibrate Real Time Air Pollution data against the nationally released air pollution data. The data will be included in the Citi Logik app, and it is hoped that this will allow planning teams to compare the data with real time transport information. They will then be able to make decisions at both the strategic and citizen level.

Citi Logik's solution also includes pollution monitoring. So, by using data captured on Citi Logik sensors placed around the city, the Council can calibrate the information received from DEFRA sensors and build an accurate and complete view of the pollution levels. In the future this will help the teams report on pollution, see patterns and take the right action to manage traffic and planning changes in real-time.

Ian Anderson, director of legal services and partnerships at the Hull City Council, says that the adoption of Citi Logik's Analytics software supports the implementation of the city's smart city vision:

"Our Smart Digital Strategy is ambitious and brings together multiple initiatives. There are not many examples where a city has taken time to build a viable plan to transform how services are delivered cohesively. It is therefore important to have the support of a company with the skills and understanding to translate available big data into a form that is both comprehensible and useable in the context of traffic management and planning. Citi Logik's heritage in this field is invaluable."

Ian adds that Citi Analytics is supporting delivery of the vision on a number of levels: "The Citi Analytics solution provides the city with real time data in relation to the flow of traffic along main routes into and through the city and the ability to interpolate that with the real time impact on air pollution. It also provides the data analytical tools to understand the origin and destination of journeys into the city, for both normal daily travel and major events, supporting longer term transport and city planning, which will be essential as we move towards implementing the city's separately procured Smart City Platform." ■

Introducing the critical comms column

Mladen Vratonjic, chair, The Critical Communications Association (TCCA)

How would you define critical communications? There are many instances where needing to communicate is important. But truly mission critical communications can mean the difference between life or death.

This is the first in a series of articles where we will take a look at the critical communications landscape around the world, how it is evolving to meet the changing needs of the end-users, and the huge amount of work that goes on behind the scenes – largely carried out by volunteers – to ensure that critical communications networks are robust, reliable, resilient and secure. It is those networks that support, amongst others, our first responders - the police, medical and fire and rescue services that we rely on to help us in a crisis and keep us safe.

Until very recently, the networks that supported critical users were specific to that sector, designed from inception to meet the unique needs of mission critical users. The technologies – TETRA, P25, DMR, Tetrapol – have resilience and security built in from the very beginning, both in the infrastructure and the devices, in hardware and in software, in order to deliver trusted, reliable and resilient communications support. However, they are all narrowband technologies and as such are limited in the type of data applications they can support.

As any of us who use a smartphone will know, in the consumer mobile communications market, the focus is firmly on data applications. Although the past year has seen a resurgence in the use of voice calls due to the pandemic, overall the mobile networks are supporting mostly data-centric applications, and the same evolution is coming to the critical communications world.

While voice will always remain an essential – and the most immediate – form of communications between first responders in a crisis, there is a need for broadband networks to have the capability to be mission-critical bearers for mission-critical data – to have a similar level of reliability, resilience and security as the dedicated narrowband critical communications technologies.

This is the challenge that is being addressed around the world, as governments look to ensure their first responders have the best possible communications tools with which to carry out their critical work. The way forward however is very much dependent on the availability of spectrum and of course the level of investment that each country or region is able to commit.

Two examples: In the US, FirstNet is the new nationwide broadband communications platform for data, built for the country's first responders and extended public safety community. It is based on a public-private partnership with telecoms operator AT&T, and uses spectrum set aside by the US government specifically for FirstNet. The existing narrowband networks that carry critical voice services continued to be used for the meantime. In the UK, the Emergency Services Network (ESN) is being created using the network and spectrum owned by commercial mobile network operator EE. An ambitious roll-out schedule needed to be revised more than once to ensure that the ESN will be as trusted as the existing TETRA-based Airwave service before that network is switched off and ESN becomes the first responders' communication platform for both voice and data.

The US and the UK are two of the countries that are the most advanced in terms of delivering critical broadband. Other countries are at various stages from consultation through to procurement.

It is not just the networks that need to be 100% trusted. The services – voice, data, video – and the devices all need to work seamlessly. To achieve this, the Third Generation Partnership Project (3GPP) has been developing a set of standards for mission-critical functions for broadband networks. Currently, these are Mission Critical Push-to-Talk (MCPTT), mission critical data (MC Data) and mission critical video (MC Video). This time these are not specialised, dedicated standards for mission critical systems but rather parts of the mainstream standards of cellular telephony, for 4G and 5G networks, developed and included on the basis of requirements and with the support of the critical communications community. When services are created to those 3GPP standards specifications are they considered to be mission critical.

For devices, work is ongoing with the Global Certification Forum (GCF) to develop a testing and certification process to ensure user devices can also be termed mission critical whilst conforming to the 3GPP standards and being interoperable with networks and other devices built to the same 3GPP standards.

Against the backdrop of all the work going into developing mission critical broadband, the trusted narrowband networks remain in full use, new networks are being implemented and existing networks upgraded and refreshed. TCCA works closely with standards development organisation ETSI to ensure the TETRA standard is enhanced to support users to 2035 and beyond.

It is estimated that the transition from narrowband to broadband mission critical networks will take perhaps more than ten years. It is anticipated that in the meantime, many organisations will use hybrid mission critical networks and that it is necessary to enable interoperability and collaboration of narrowband and broadband networks and devices. Therefore, 3GPP on the one hand and ETSI on the other are working to develop a standardised interface for their interconnection.

TCCA, on behalf of its members represents all standard mobile critical communications technologies and complementary applications. Our members design, manufacture, build, implement, utilise, analyse, promote, develop and deploy critical communications. We believe in and promote the principle of open and competitive markets through the use of open standards and harmonised spectrum, working with stakeholders in the critical communications ecosystem to achieve this.

There are many, many organisations and individuals committed to ensuring that critical communications networks and services are the best they can be. We will endeavour through this column to showcase some of the initiatives, to discuss the challenges and the expectations, and to hopefully encourage more people to become involved in shaping the future of critical communications.

Optimising cooling within the data centre

Alex Thompson, sales engineer, technology sector, Airedale International

The world has been catapulted into a virtual reality at a much faster pace than we ever envisaged and the need to move our day to day lives online, in response to the pandemic, has seen the data centre industry having to respond fast to maintain service and match demand.

Since the age of computers began, the need for effective cooling to keep IT operational has been a much debated topic. At Airedale, we invest heavily into R&D to ensure we meet the objectives and solve the issues faced by data centre managers, both at strategic and operational level. With a wealth of expertise in this field, we can share some of our frequently covered topics of discussion and resolutions.

Perhaps frustratingly, there isn't a one-size-fits-all solution to data centre cooling. Every operation is different and power/ cooling load, physical footprint and geographical location of the data centre will always impact on the critical cooling solution employed, but there are some common themes to consider that will assist with decision making and here we look at 3 key points.

1. **Aisle Containment:** Historically, data centres were cooled using CRAHs (computer room air handlers) to cool the general space. However the issue with this is that it resulted in hotspots, leaving some crucial areas unable to be cooled due to poor air distribution. By employing a more strategic server layout, hot exhaust air can be segregated within specific aisles, with cool air channelled towards the servers that need it. Ensuring server intake cool air and the exhaust hot air do not mix increases the efficiency of the system, whereby hot air is returned to the CRAH (making them more efficient) and cool air can be directed to the servers as required. This separation of "conditioned air" from "returning exhaust air" is a crucial first step for optimising efficiency.
2. **Energy Efficiency:** Cooling a data centre consumes a significant amount of energy and efficiency is key to ensure minimum waste, to reduce carbon footprint and minimise lifecycle costs. Free Cooling chiller technology, which is the process of using external ambient temperature to reject heat in a chiller, rather than using the refrigeration process, is a highly effective method of reducing waste and operational costs. If used within an optimised system, free cooling can provide significant energy savings. It can take effect when the difference between the outside supply and return temperatures is as little as 1°C. This means that, in a 24/7 data centre with a typical server inlet temperature of 24°C, over 95% of the year can be spent with free-cooling active. Other energy efficiency measures can also be employed alongside free cooling, such as part-load operation for when full capacity isn't demanded by the servers, thus reducing energy consumption in line with IT demand. Airedale's DeltaChill Azure, which uses the lower GWP refrigerant R32, provides one such free cooling solution.
3. **Intelligent Controls:** Investing in technology can only be effective if its operation is monitored on an on-going basis. Intelligent controls that offer 24/7 demand adjustment for precision control of temperature, airflow and air pressure difference to maximise uptime and optimise efficiency. Airedale's Helix control can work in conjunction with the data centre infrastructure management (DCIM) system to ensure continuity across the whole site. Within the controls system, any leakages, failures and downtime can be quickly recognised and within systems that employ an N+1 or N+N redundancy strategy, downtime is minimised.

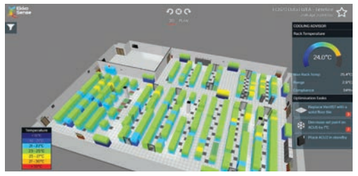
So whilst there is no standard fit, an example solution for a 750kW Data Centre might be to select 3no chillers, such as the DeltaChill Azure, with two chillers providing 382kW cooling and the 3rd chiller providing N+1 resilience. These would work alongside 4no downflow AHUs, such as Airedale SmartCool chilled water units each providing 187.25kW, supplied via a floor void with contained hot aisle and ceiling void return to CRAHs. To mitigate risk of failure, controls could be available on circulation pumps to ramp up pump speed in the event of a CRAH failure and overcome the increased coolant pressure drop. This system described, offers an annualised Efficiency of 11.0 (i.e. 11kW of cooling per 1 kW of power) with a partial PUE (Chillers + CRAH) of 1.091*.

There are many day to day aspects of the data centre operation that need to be considered when it comes to developing a cooling strategy. It is important to consult with an experienced cooling team who can identify risks and advise on design to maximise efficiencies within the setting. At Airedale we have dedicated teams established to work with both enterprise, edge and large data centre operators, to develop the most appropriate and advanced solutions for our clients.

**All the above partial PUE figures are based on set parameters and do not take into account any other inefficiencies (other power losses)*

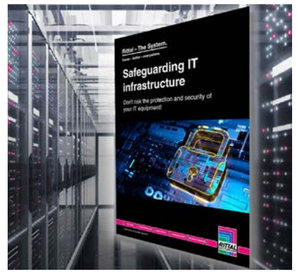
PRODUCTS

EkkoSense Cooling Advisor provides data centre operations teams with focused cooling performance recommendations and advisory actions. Built right into the heart of its 3D visualisation and analytics software, Cooling Advisor is the industry's first embedded advisory solution. It helps organisations to unlock significant data centre cooling energy savings – just by acting on the software's advice alone. Cooling Advisor's actionable changes – such as suggested optimum cooling unit set points, changes to floor grille layouts, checking that cooling units are running to specification, fan speed adjustments or advice on optimum rack locations – are based on powerful AI and machine

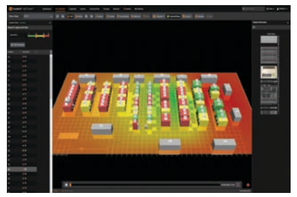


learning analytics. Recommendations are presented each time for human auditability before team members make the suggested changes. They can then use EkkoSense's data centre performance optimisation solution to confirm that Cooling Advisor recommendations are delivering the expected results. With the latest software from EkkoSense already unlocking data centre cooling energy savings of up to 30% per annum, Cooling Advisor goes one step further. It provides clear recommended actions that take advantage of EkkoSense's PhD-level optimisation expertise to equip data centre teams with a powerful self-optimisation capability. By adopting analytics and machine learning, EkkoSense ensures that Cooling Advisor delivers advice that is specific to each data centre room. This approach recognises that data centres never stay the same. Using Cooling Advisor and following its recommendations will allow operations teams to unlock a further 10% saving on their data centre cooling costs. Additionally, by deploying cooling duty sensors to track cooling loads, EkkoSense is also able to identify undetected cooling unit faults before they are even picked up by BMS alerts. By capturing entirely new levels of data centre cooling data, including energy usage and airflow distribution, EkkoSense is also able to map zone-by-zone cooling analytics within the data centre to help with resiliency and capacity planning decisions. The application of analytics and machine learning here will show which AHU units are servicing which racks, allowing Cooling Advisor to identify which AHUs could be put into standby or turned down if using variable speed fans. *ekkosense.com*

IT professionals are coming under increasing time pressure and managing increasingly complex systems. With its new TX CableNet, **Rittal** is accelerating professional-quality network cabling. Even large quantities of cable with a soft bending radius are easily inserted, and perfect cable routing is achieved with the "waterfall principle". The pre-assembled open-frame design with a pitch pattern for Rittal accessories ensures speedy assembly and easy maintenance. For standard orders from stock, Rittal promises express delivery. IT managers are having to expand and manage increasingly interconnected networks at a rapidly growing rate. When it comes to components, speed and reliability are needed in several ways: "In the TX CableNet, we have combined innovative cable management with the demand for professional quality," explains Emma Ryde, Rittal's Product Manager for Industrial and Outdoor Enclosures "Besides the mechanical properties of the rack, this includes a systematic approach, reliable cross-regional availability and rapid delivery." Right from the start, the new TX CableNet has been designed as a network rack and it is intended for perfect cable routing with fast installation. The following principle applies even with large quantities of cables: simple insertion instead of laborious pulling. This is ensured by recesses with rounded edges on both sides and over the entire depth of the roof. The outer cable routing struts on the roof edges are easily removed, the complete cable harness is inserted and the struts are then securely hooked back in place again. This way, even large cable harnesses slide down from the roof and in a soft bending radius into the distributor in no time at all. Thanks to this "waterfall principle," the cable routing follows the best practice method for copper cables and for fibreglass optic cables. The open frame construction also permits the entire depth to be used when feeding in via the floor. *rittal.co.uk*



Sunbird DCIM makes it easy to improve data center efficiency, enabling you to safely increase utilization of existing capacity and reduce costs without risking downtime.



With Sunbird's remote data center management solution, you can: Increase utilization with automatic power capacity planning that can achieve 40% greater utilization of cabinet resources, intelligent capacity search that finds the optimal space to deploy equipment for you, and 3D floor map reports to analyze multiple cabinet capacity parameters at the same time. Report on KPIs such as PUE, see trends in real-time, and monitor all capacities with 100+ interactive, zero-configuration dashboard charts and reports. Design your physical infrastructure for optimal efficiency before the build out. Automatically create 3D rack diagrams with asset details and visually account for aisle containment, floor PDUs, and cooling infrastructure. See site-by-site available power and data port capacity by port type with a vast vendor models library that provides the correct port count and specifications for every device. Monitor energy consumption by collecting, storing, and reporting on real-time power data across the entire power chain as well as temperature and humidity sensor data. Set thresholds, receive alerts, and make appropriate modifications if power consumption reaches warning or critical levels of circuit capacity. *sunbirddcim.com*

Airedale's SmartCool I Drive is a highly efficient indoor precision cooling unit that provides critical cooling to IT equipment, making it ideally suited to data centre applications and low, medium and high density computer room cooling applications. Optimised for high return air temperatures and ideal for hot and cold aisle containment, the range is perfect for the 24/7 operation of sensitive systems in critical application environments. With a wide outdoor ambient envelope (-20˚C up to +50˚C) and the capability of longer pipe runs, allowing outdoor condensers to be up to 100 metres from internal units, the SmartCool™ I-drive allows for flexible installation without compromising efficiency or performance. Inverter driven compressors enable precise control of supply air temperature (+18˚C to +26˚C), varying their running speed to adjust to expected or unforeseen load variations, resulting in increased efficiency and a wider operating envelope. SmartCool I Drive comprises of two optimised capacity selections for traditional and high return air temperatures, suitable for periphery cooling and aisle containment applications respectively. Available in 4 case sizes, all SmartCool I Drive units are single circuit DX aircooled with either one single inverter driven compressor (X100) or a tandem compressor set (X200). The incorporation of inverter compressors enables exact control, superior efficiency and performance. It is a system prepared for every eventuality, responding to unexpected load variations to deliver market leading cooling density. " *airedale.com*

Companies of all stripes are undergoing digital transformations, increasingly relying on technology to run nearly every aspect of their business. As a result, they are creating more data that needs to be processed and stored, which requires a data centre. Legal requirements, the need for local data consolidation and, above all, the high network costs, latency and network security have led to an enormous growth in decentralized IT, or so-called edge applications. A specific challenge for these environments, is the use of rooms in buildings that were not designed for the operation of IT equipment. That's where a cabinet-sized micro data centre can be deployed, to ensure that IT operations are comparably as reliable as in a large data centre. Also, since edge IT applications usually do not have qualified staff on site, easy remote monitoring and management of all infrastructure elements is important. The Vertiv VRC-S is the ideal micro data centre solution for such applications. It is fully factory assembled and designed specifically for IT edge applications. Available in various configurations, the highly-efficient Vertiv VRC-S is delivered in days and installed in hours. Choose from four different cabinet sizes with two separate cooling methods (split and self-contained) with back-up, and the option of integrating a UPS. Plus, an intelligent switched PDU, including monitoring of all components, and a comprehensive software package completes the offer. You get a plug-and-play IT solution that reliably and efficiently satisfies your edge IT requirements. *vertiv.com*

Please meet...

Andy Aplin, director sales and engineering for EMEA & LATAM, Netskope

What was your big career break?

I know I really should say that joining Netskope, nearly seven years ago, as Director of Sales and Engineering for EMEA and LATAM was my big career break, but looking back over my 25 year+ career, I would have to say becoming one of the first Cisco Certified Internetwork Experts (CCIE) in Europe back in 1997, was a key moment. At the time, and still today, CCIE accreditations were accepted worldwide as one of the most prestigious networking certifications in the industry. It was a door opener to establish myself as a leading networking guru. Having the accreditation enabled me to get my first role in a start-up vendor. I joined CacheFlow as its first Systems Engineer in Europe. CacheFlow later rebranded to Bluecoat and was acquired by Symantec in 2016.

Who was your hero when you were growing up?

I am a huge motorsport fan and have grown up watching Formula 1 (F1). For me, nothing beats the excitement of watching cars that have been designed to a hundredth of a millimetre /or gram, race up to 200mph around a track where the limits are so close, any slight movement could result in a disaster. Former F1 World Championship winner, Nigel Mansell, is one of my hero's. No driver fought harder to get into F1 and few fought harder when they got there. Mansell was determined, aggressive, daring and one of the most exciting drivers to watch. He physically wrestled his cars around the track. Mansell left a lasting impression on me, showing how determination and persistence would deliver ultimate success.

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

It may seem obvious from my previous answer - it would have to be the Automotive industry. I am a petrol head through and through. If I was choosing a career path now, it would be mechanical engineering, rather than computer science where I started.

What would you do with £1m?

I would invest it in property. Maybe even stretch to one of the properties at Escapade Siliverstone(!), but only because I can't buy public stock in Netskope…yet…

Where would you live if money was no object?

Wow, what a thought! My dream would be to split my time between the UK and Italy. I would always have roots in the UK as this is where I grew up and where my family is. But, to be able to also plant roots in Italy would me amazing. I try to travel to Italy regularly (obviously not managing that with the current travel restrictions). The Northern Italian lakes are my favourite part - Lake Como is particularly special to me. I once stayed in a hotel room from which Sir Winston Churchill painted the lakes. It is said that Italians have mastered living happily because they have perfected the blend of food, family and good humour. They could be right, I certainly love the food, wine and family-centric life that is associated with the Italian culture. And of course, the more reliable sunny summers.

The Beatles or the Rolling Stones?

The Beatles every time. Lennon and McCartney's lyrics capture so many emotions and provoke so many memories. Although the songs were written from their experiences, people can interpret them in a way that's personal to them - that's the magic that makes their music timeless and so well loved across generations.

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

I was fortunate to be given this advice early in my career, and it has kept me in good stead ever since; "Always treat people the way you like to be treated and lead by example." I can't say that I have succeeded in always following the advice, but it's definitely a code I try to follow and something everyone should bear in mind.

If you could change any law, which would it be?

I would like the UK to mimic some states in the USA and allow people to drive from the age of 16. It may not be right for everyone, but it would have meant that I would have avoided riding motorbikes and got straight on to driving cars. Like many other teenagers, at 16 years old, I thought I was invincible on 50cc moped. Only time would teach me that ice and skinny wheels are not a good mix, especially when combined with not looking where I was going. Unfortunately, the car in front marked the end of the road for me.

What will you miss about Donald Trump?

Donald who …..?