FEBRUARY 2021
networkingplus.co.uk

NETWORKING+

Production scale in IoT

Key considerations ahead of an IoT production rollout

Nick Sacke, Comms365, *p7*

Privacy impact in digital era

Why data privacy is a priority for many organisations

Zack Zilakakis, Juniper Networks, *p13*

Questions & answers...

Networking+ chats with the co-founder of cloudDNA

Al Taylor, cloudDNA, *p16*

Shared Rural Network boost for UK enterprises

The first phase of the new Shared Rural Network (SRN) provided by O2, Three and Vodafone, could increase the turnover for rural businesses by £187.7m per annum in addition to providing more reliable connectivity, according to a new study commissioned by O2.

All three mobile operators are working to build and share 222 new 4G (mobile broadband) masts in order to help resolve partial not-spots, including 124 new sites in Scotland, 33 in Wales, 11 in Northern Ireland and 54 in England. Not-spots are usually areas where only one provider is available. The construction phase for these will begin this year, but it will take until 2024 before completion.

O2 said this first phase alone will raise the proportion of the UK with access to 4G networks from 67% to 84%. In assessing the impact of this O2 commissioned Development Economics to model the benefits for rural businesses and individuals.

The new report found that, once the first phase of the rollout has been completed, rural businesses located near new mobile mast sites could benefit from an annual increase in turnover of £187.7m. Access to the SRN for individuals and businesses will also allow these rural communities to contribute an extra £58.9m to the UK economy (GDP) each year.

Moreover, the report noted that the largest share – some 28% – of the gains in business turnover and productivity are expected to occur in rural Scotland, valued at £79m in additional business turnover and a £24.1m added contribution to the UK economy. This is followed by Northern Ireland, which will see 16% of the predicted net gains, south west England with around 15%, Wales with 14% and the north west of England with 8%.

It was also revealed that 42% of the projected increase in turnover will benefit those in the struggling hospitality sector, covering rural distribution, hotels and catering businesses, which are in line for a £78.8m boost to revenues. The other sectors that account for the largest shares of the increase in turnover are expected to be transport and communications (17% of the predicted revenue increase) and professional, financial, property and business services (10% of the increase).

continued on page 2

Register for Networking+

SRN boost for UK enterprises

Continued from page 1

David Samuel, managing director at communication technology vendor 24 Seven Cloud told *Networking+* that networks "all finally sharing infrastructure is positive news", but what is unclear is how it will work in practice and what the results will look like. "O2 and Vodafone have been sharing masts for a few years now and blackspots (or not-spots) still exist," he added. "Any improvement however for the consumer is only a good thing and will go further to support connectivity for remote/WFH users and unified communications platforms."

The last year proved that reliable mobile connectivity has been essential for keeping us all connected to our loved ones and keeping businesses across the UK up and running – and 2021 is set to be no different," said Derek McManus, COO at O2. "Our latest research shows that mobile has the power to make a real, positive difference to people in rural communities and demonstrates the difference we can make when operators, the government and Ofcom work together to achieve a shared objective."

McManus added that it remains "extremely difficult" to accurately assess the economic benefits of improved mobile connectivity, particularly in areas like partial not-spots, where an existing service may already exist from a single operator. "Otherwise, the SRN aims to provide guaranteed coverage to 280,000 premises and 16,000km of roads and boost 'in car' coverage on around 45,000 km of road and better indoor coverage in around 1.2m business premises and homes," he said. ■

NetUtils launches 'Platinum Tier' managed cyber security services

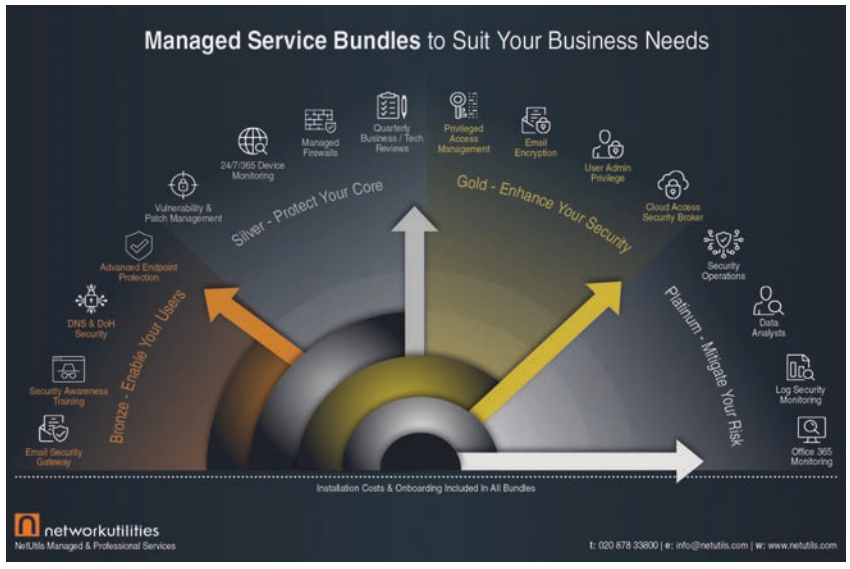
IT specialist NetUtils has launched what it describes as one of the UK's most advanced and highly-integrated managed cyber security service aimed at helping larger enterprises to improve cyber security defences while reducing operational cost and complexity.

The new "Platinum Tier" includes a fully-staffed, 24/7 Security Operations Centre (SOC), is backed by NetUtils continued certification around the ISO 9001 and ISO 27001 standards and as a registered Crown Commercial Service supplier.

Furthermore, this top tier service offers key elements a large enterprise should deploy based on best practice methodology and includes Advanced Endpoint Protection, Vulnerability & Patch Management, Managed Firewalls, Email Security Gateway, Privileged Access Management and Cloud Access Security Broker capabilities.

The built-in SOC services provides full-time security monitoring across devices and applications including Office 365 along with structured Security Awareness Training sessions and ongoing helpdesk service.

"Larger enterprises are faced with the dual challenges of managing more remote staff while still trying to deliver the core IT projects that are critical to the business," said Ashok Thomas, CEO for NetUtils. "Our Platinum Tier Managed Cyber Security services are based on feedback from several enterprise customers around what they need - and is effectively a formalisation of a number of disparate services that we have been delivering successfully for many years."



The new "Platinum Tier" includes a fully-staffed, 24/7 Security Operations Centre (SOC), is backed by NetUtils continued certification around the ISO 9001 and ISO 27001 standards and as a registered Crown Commercial Service supplier

NetUtils is the most certified Juniper Networks partner in Europe and maintains over 420 industry and vendor accreditations within its team including CISSPs and CISMPs, Fortinet's NS7, and Juniper JNCIPs. IAs part of the managed cyber security services launch, NetUtils has invested over £1.2 million adding more staff, enhanced training and additional data centre capacity to meet growing demand.

The new Platinum Tier managed security services also aims to address several challenges that have accelerated due to the ongoing pandemic including critical digitisation projects, reduction in IT budgets and ongoing cyber security skills shortage ■

Truespeed announces full fibre roll-out in Bath and environs

Truespeed has started rolling out its ultrafast, gigabit-capable full fibre broadband network in Bath, propelling the World Heritage city into the gigabit era.

The Bath-based firm is also expanding its footprint into neighbouring areas in Somerset including Keynsham, Saltford and South Widcombe. In Wells, where the Truespeed build began in earnest in June 2020, Truespeed has now passed over 3,000 premises. Today the firm has announced that it is boosting its investment in Wells, with plans to connect more areas of the city and continue expanding its current building works in surrounding areas such as Wookey and Coxley.

Wera Hobhouse, MP for Bath said: "Truespeed's investment will benefit the city enormously as ultrafast broadband connectivity can't come soon enough for Bath businesses and residents. It's great that a Bath-based firm is at the forefront of supporting our communities and taking our beautiful city into the full fibre fast lane."

Truespeed also offers primary schools and community hubs passed by its network free ultrafast broadband for life. To date, over 100 schools and community hubs have signed up.

"We're excited to get going in Bath while stepping up the roll-out of our full fibre network in Wells and surrounding areas in Somerset," added Evan Wienburg, CEO of Truespeed. "We're lighting up our map of the South-West and bringing under-served households and businesses the future-proofed gigabit capable connectivity they deserve." ■

Truespeed has announced that it is boosting its investment in Wells, with plans to connect more areas of the city and continue expanding its current building works in surrounding areas such as Wookey and Coxley

CityFibre starts Bradford's full fibre transformation

Bradford in Yorkshire is marking a major milestone in its digital transformation as work begins to extend its full fibre network to reach almost every business and home in the area.

As part of a £75m private investment from CityFibre, Bradford will benefit from the city-wide full fibre network roll-out, meaning enterprises will soon be able to enjoy access to the faster and more reliable connectivity.

According to research from economic consultancy Regeneris, full fibre connectivity will have a major impact in Bradford over the next 15 years. It shows that up to £136m could be added to the value of local homes, while smart City initiatives could add as much as £95m locally. Access to full fibre could also unlock £69m in business productivity and innovation, while a further £40m in growth could be driven from new business start-ups, with enhanced connectivity making it easier and less expensive to set up base and run efficiently.

Construction work has officially commenced in East Bowling, with the rest of the city set to follow over the next four years. Network Plus is delivering the construction programme on CityFibre's behalf, using modern build techniques to deploy the network quickly. The team is also working closely with CityFibre, Bradford Council and local communities to manage disruption and ensure a fast and successful roll-out. Meanwhile, residents are being kept informed by mailings ahead of works in their streets.

"Bradford is one step closer to becoming a Gigabit City with the commencement of work to install state-of-the-art digital infrastructure across the city, said "Kim Johnston, city manager for Bradford. In addition, it will provide growth opportunities and a platform to support businesses to take their products or services to a national and international audience."

Councillor Alex Ross-Shaw, portfolio holder for regeneration, planning and transport, at Bradford Council, added: "Fast and reliable broadband is so important in the world today, from facilitating digital on-demand content to supporting businesses to grow and flourish." Currently, fibre-to-the-premises (FTTP) is available to less than 20% of premises across the UK.

Once activated, services will be made available from an increasing range of broadband providers. ■

EDITORIAL:
Editor: Robert Shepherd
roberts@kadiumpublishing.com
Designer: Sean McNamara
seanm@kadiumpublishing.com
Contributors: Gerry Moynihan, Jürgen Hatheier, Rich Turner, Nick Sacke, Robin Farnan, Zack Zilakakis, Martin Blunn, David Samuel, Al Taylor, Steve Burden Hugo McGuire

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

Company © 2021. All rights reserved. The contents of the magazine may not be reproduced in part or whole, or stored in electronic form, without the prior written consent of the publisher. The views expressed in this magazine are not necessarily those shared by the editor or the publisher.

ISSN: 2052–7373

Virgin Media Business teams up with Zscaler

Virgin Media Business (VMB), the network and communications solutions provider, has boosted its cloud security offering with the addition of the Zscaler service portfolio.

Driven by the global Zero Trust Exchange Platform, Zscaler's cloud-native platform provides an integrated cloud security service that sits between an enterprise's users and corporate applications and networks.

The Zscaler Zero Trust Exchange is also said to facilitate a secure connection between users, applications and devices over any network, in any location, helping accelerate cloud adoption and hybrid working strategies and boost productivity while reducing risk and costs.

Partnering with Zscaler allows VMB to enhance its SD-WAN, hybrid cloud and cloud security solution suite by offering globally leading service that encompasses the SASE framework. The cloud-native technology offers a range of security services, like Secure Web Gateway, Cloud Firewall, Cloud Sandbox, CASB, Cloud DLP and secure remote access functionality without the challenges that on-premises equipment often present, making it perfectly suited to businesses looking to protect their data with a dispersed or remote workforce.

The Covid-19 pandemic has forced many organisations to shift people and operations outside of their core networks, with fewer employees working from HQ or branch sites. With traffic entering corporate networks from remote locations, this has created additional security challenges for organisations to manage.

Zscaler Private Access directs traffic to the Zscaler Zero Trust Exchange using Zero Trust Network Access to limit application access to authorised personnel only.

This means that regardless of a user's location, organisations can securely access any cloud, private or public service on the back of cloud-based security policies and with corporate acceptable user policies in place, to greatly improve flexibility, scalability and security when compared to traditional VPN network access.

Working across WAN, IPVPN, SD-WAN, mobile and even public internet connections, the Zscaler Zero Trust Exchange can help accelerate moves to the cloud. Organisations can benefit from flexible, scalable services while also reducing capital expenditure and simplifying corporate security policies and on-premises equipment.

Zscaler's cloud-native platform provides an integrated cloud security service that sits between an enterprise's users and corporate applications and networks

Sean Sullivan, director EMEA channels at Zscaler, said the company was "looking forward" to the partnership with VMB to accelerate the latter's customers' secure journey to the cloud. "By bringing network, application and security requirements all together in one SASE framework, our Zero Trust Exchange Platform enables them a smooth transformation journey from on-premise security to the cloud," he added. "With more and more apps being consumed in the cloud and increasing workforce mobility, the market is coming to Zscaler and Virgin Media Business is well positioned to answer the customer demand for user-friendly and next-generation security." ■

Dubber achieves compliance call recording certification

Dubber said its Unified Cloud Call Recording service has achieved compliance call recording certification for Microsoft Teams.

The firm said to be certified under the Microsoft programme, companies are required to submit their services for third-party approved testing for quality assurance, performance within the Microsoft Azure environment, interoperability and compatibility with the Teams user experience, security and compliance, marketing and customer support.

Certification for the Dubber Unified Call Recording (UCR) solution means service provider partners, channel partners and enterprises are ensured of a trusted solution that has met the highest levels of testing for the Teams platform.

James Slaney, co-founder and COO at Dubber, said that Covid has driven working from home and a rapid increase in demand for UC solutions such as Microsoft Teams. "The grace period granted by the FCA on meeting certain compliance mandates - including recording of calls - is now over, driving a new need for compliant unified call recording," he told Networking+.

Spanning several months of rigorous testing, Dubber said its solution met and exceeded the parameters of the certification process for voice, video and screen share. As a part of the certification process, Dubber will also be included in the Microsoft AppSource Marketplace for compliance. ■

Register for Networking+

FROM THE COVER

Hiding in plain sight – why IT complexity is a hacker's dream

The saying 'can't see the wood for the trees' is apt when talking about cybersecurity. Complex IT environments are a cybercriminal's dream; they are typically harder to monitor and secure, and as a result, easier to breach. The rise of homeworking has led to more devices being connected to corporate systems than ever, and a proliferation of cloud services reshaping IT environments. Cybersecurity risk management is becoming a bigger priority; 46% of organisations in a recent survey we conducted deemed it an essential part of a homeworking strategy. But what do organisations need to focus on to improve cybersecurity in complex IT environments?

Cut through the complexity

Cybercriminals are increasingly sophisticated at targeting weaknesses, making it essential for organisations to cut through their IT complexities and identify all potential vulnerabilities. However, IT environments are more complex, and this is increasingly difficult to do, requiring fulltime cybersecurity professionals when skills are in short supply. If organisations are to stay ahead, they need to take a tech-led approach to cybersecurity.

Implementing a **security information and event management system (SIEM)**, is a great start, as it gathers intelligence across on-premise and cloud environments. Solutions like Azure Sentinel can monitor every corporate device and user, alerting IT teams to suspicious activity or compromised systems. Early detection is critical in helping minimise the impact of a breach.

But a good SIEM isn't enough to provide complete security, businesses need core security systems such as **antimalware protection and data backup**. All-in-one security solutions such as Acronis provide backup and security to cover mobiles, laptops, desktops, servers and virtual machines, alongside cloud suites such as Microsoft 365 and Google Workspace.

By using an integrated solution, organisations can eliminate complexity and deliver new security capabilities while reducing costs. Acronis, for example, lets organisations mix and match options across their IT estate for a solution that protects everything they need, in the best way. Beyond the fast, reliable recovery of applications and data, such solutions also offer next-generation security based on AI and machine learning for added protection.

With digital transformation continuing at pace as a result of the pandemic, IT complexity will only increase. However, by using the right combination security solutions, organisations can keep their IT environments secure without having to hire huge workforces.

At Daisy, we help businesses with these challenges daily. Get in touch with our team at **dcs.tech/contact-us** to see how we can help.

By Steve Burden, security product manager at Daisy Corporate Services

Halfords deploys 8×8 solutions

UK motoring and cycling retailer Halfords has expanded its deployment of the 8×8 cloud contact centre and communications product to enhance communications and customer experience. The firm decided to unify communications and contact centre operations across its three main business divisions – retail, automotive and mobile services. Gareth Brophy, head of customer support at Halfords, said: "Partnering with 8×8 and deploying an integrated cloud contact centre and communications product, enables us to deliver a customer-first strategy, and scale our operations to drive efficiency and profitability."

Wellcome Sanger Institute embarks on cost-saving energy efficiency drive

The Wellcome Sanger Institute has called on tech partner EfficiencyIT to revamp its energy monitoring and management systems at its data centre near Cambridge. Home to Europe's largest genomic datacentre estate, the server farms it contains play a vital role in supporting the firm in advancing the scientific community's understanding of how DNA affects human health and well-being. The project will see EfficiencyIT deploy more than 300 custom-designed APC by Schneider Electric Rack Power Distribution Unit (PDU) metering systems at the on-premise data centre.

IT vacancies up 52% in second half of 2020

Despite the impact Covid-19 has had on recruitment activity, professional IT vacancies fared considerably well in the second half of 2020, with the number of jobs available rising 52% when compared to the first half of the year. That's according to new research from the Association of Professional Staffing Companies (APSCo), the trade association for the recruitment sector. The data, provided by business intelligence specialist Vacancysoft, revealed that the increased requirement for tech professionals to keep Britain working, learning and connected during the pandemic resulted in demand for IT talent intensifying between the first and second half of the year rising by 52%.

Colt DCS operations go 100% green

Colt Data Centre Services (DCS) said its operations across the UK and Europe are fully powered by 100% renewable power. The data centre provider has also committed to providing green power to sister company Colt Technology Services and its customers using DCS data centres in the region, in an effort to help them also reduce their own carbon emissions. Across the UK and Europe, Colt DCS currently operates 17 carrier neutral data centres, with three in London."Our accelerated transition to renewable energy is just the first step in our journey to becoming more sustainable as a business and industry, with much more to come," said Colt DCS director of energy and sustainability, Scott Balloch.

Leading UK estate agency Foxtons suffers major hack

UK estate agency Foxtons Group suffered a major data breach in October 2020, enabling hackers to steal personal and financial information before posting it on dark web forums. The major data breach forced the company to temporarily shut down its customer portal, MyFoxtons. Although Foxtons claimed that no sensitive data was compromised as a result of the attack, its employees were reportedly unable to access customer and landlord contact details on company systems. The agency later confirmed that Alexander Hall, its mortgage broking business, was affected by the data breach. iNews reported that more than 16,000 card details, addresses and private messages were stolen from Foxtons' systems and uploaded on the dark web.

Danish cybersecurity firm opens second UK office as part of expansion plans

Danish cybersecurity firm Heimdal Security has opened a second UK office and signed a new long-term distribution agreement as part of an aggressive expansion which will make the UK its biggest global operation. The new office in Leeds is within easy reach of Yorkshire-based Brigantia, its master distributor in the UK and Ireland. Heimdal, which currently employs 30 staff in Leeds and London, expects to more than treble that in the year ahead – outstripping the size of its teams in Copenhagen and Romania. Country manager Ruth Schofield, who heads up the UK business, said: "Heimdal is an exciting, disruptive company whose technology takes endpoint protection to the next level. Rather than just detecting and blocking threats, it seeks them out in advance. It's like being on the door at a nightclub – we're not just stopping the wrong people from entering but going outside to check who's in the queue." Heimdal said its cybersecurity suite will soon cover remote access.

MLL Telecom partners with TKAT

MLL Telecom has secured a seven-year contract with The Kemnal Academies Trust (TKAT) to provide high speed broadband services as well as firewall and content filtering. TKAT is one of the largest multi-academy trusts in the southeast of England, with 45 primary, special and secondary academies in east Sussex. The contract follows a competitive tender process under the Crown Commercial Services (CCS) Education Technology Framework Agreement, RM6103 Lot 3 Broadband Services. Kim Medhurst, TKAT's head of procurement and contracts said: "After four months the first TKAT schools are live on the new MLL broadband service". Medhurst also said that the improved broadband speed will allow TKAT to keep providing high-quality teaching.

Open book

Sunbird DCIM has compiled a list of proven tips for a successful data centre migration based on its experiences and those of its customers. For more information on 7 Proven Tips for a Successful Data Center Migration, visit: *https://networkingplus.co.uk/training-events*

Word on the web...

The network trends that will dominate 2021, according to Jürgen Hatheier, Ciena

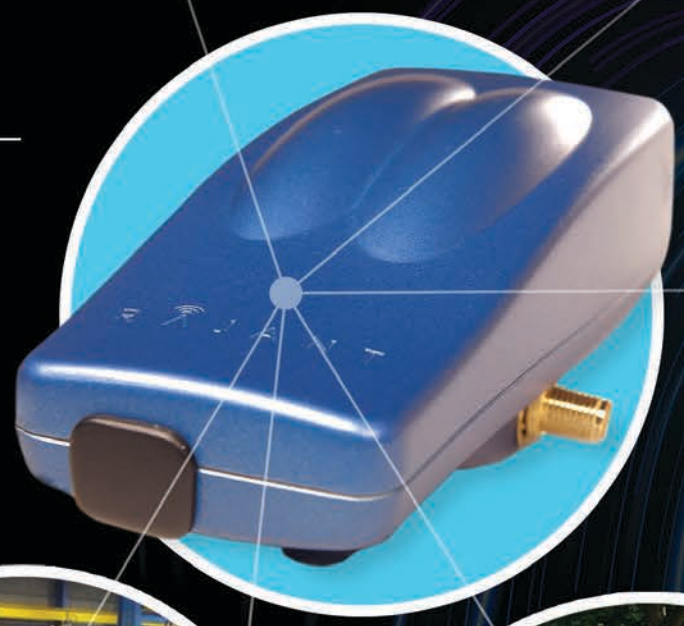
To read this and other opinions from industry luminaries, visit www.networkingplus.co.uk

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.***

RAJANT

Request a free demo at rajant.com/networkingplus

Register for Networking+

Protecting your corporate network

Cyber-criminals are targeting large organisations – and succeeding. Here's how you can stop them before it's too late, writes Rich Turner from CyberArk

Many large businesses spent last year wishing they had been better prepared: for the pandemic; for dealing with political uncertainty; and for increasing and changing security threats.

Corporate IT teams have had particular cause for concern. A 2020 report by Verizon discovered over 70% of data breaches involved victims that were large organisations, and most of these breaches were found to be perpetrated by external actors. In other words, cyber attackers are targeting corporate firms and, more often than not, succeeding.

Financial reward continues to motivate many attackers. But advanced threats also pose risk to the deep wells of data large businesses are amassing. Much of this is sensitive data, resulting in multiple negative consequences when those wells leak or are infiltrated.

The pandemic has confronted IT security teams with a continuous series of obstacles on top of the line of hurdles they already faced. With the number of challenges growing, what can businesses do to protect their corporate networks this year?

There's already plenty of conversation about whether cloud will reach its peak this year. It's easy to see why when 92% of organisations' IT environments are to some extent already in the cloud, according to an IDG report.

But all change, good or bad, brings new dynamics and new sets of diverse challenges with them. Cloud is no exception.

An increased attack surface is one of the implications of the complex nature of cloud. When traditional network perimeters are removed, the question of accountability must be asked. Whose responsibility is it to secure data hosted in the cloud? Is it the cloud provider's? Or the customer's?

Misconfiguration of account privileges is one of the most common consequences of this misunderstanding, and by extension, one of the leading causes of data breaches. When default credentials aren't reviewed, excessive permissions can allow standard users unnecessary access to sensitive data.

AI-powered automated tools that review user permissions and privileges can be of great use to IT teams trying to overcome this problem. They provide both a quick and effective way of discovering accounts with excessive privileges, and removing any superfluous permissions for specific users.

Research we carried out last year discovered that 25% of British businesses use over 100 third-party vendors. Whether consulting services or supply-chain managers, outsourcing internal functions has become commonplace.

Many of these third-party services require access to internal resources and data to fulfil their obligations. Our research found that 90% of businesses allow third parties to access critical internal resources – sensitive assets that if disrupted or stolen would cause significant harm to the organisation.

This presents a problem for IT teams, because responsibility for security is then passed to your third party partner. You may trust your own security measures, policies and protocols, but can you trust theirs?

In fact, early last year flexible office space firm Regus suffered a breach due to this exact situation, with detailed employee performance information being leaked via a third party vendor. Regus had hired a vendor to audit its staff. The vendor's security measures were weak, and the data breach was discovered in an investigation by the Telegraph. The impact an event like this has on reputation, as well as a company's finances, is deep.

This example is a warning to any business using third-party vendors. The privileged accounts of all external operators must be constantly managed and monitored. They must be secure, structured, and multi-levelled, granting third parties enough access to carry out their jobs without putting the firm at risk of a punishing data breach.

Advanced Security-as-a-Service packages are well worth consideration for businesses hoping to ease the burden of monitoring and management on their IT team.

The most evident challenge of 2020 was the transition into home offices from the traditional corporate workplace. IT teams were thrown into a maelstrom of consumer technology trying to connect to central corporate networks. Whether an employee's Wi-Fi router or their personal laptop, the huge number of new devices introduced posed an varying security risks.

This challenge is only going to continue into 2021. With the UK still under lockdown, a year in which we all work from home to a greater or lesser is easy to envisage. The security threats will have to be managed.

The approach many businesses take to this challenge adds to the problem. Far too many businesses are over reliant on security policies to keep bad threat actors out of their networks. These are almost never enough by themselves. In fact, our December research found over 50% of UK employees ignore corporate security policies. More must be done.

A lack of user-friendly processes is a common reason security policies aren't followed. Businesses may recognise the importance of security, but the processes implemented are too difficult for employees to use, creating friction in the user experience. In the end, people find shortcuts in the pursuit of efficiency and ease of use.

A balance must be struck to address this problem. Employees must first be educated on the importance of adhering to security policies, but in turn IT teams must adopt tools and processes that help minimise disruption to the wider business.

In following these tips, large enterprises will be three steps closer to being prepared for the inevitable security challenges that lie ahead.

The cloud, the increasing use of third parties, and remote work will all pose a challenge to business resilience and security. But with the right advice and investment, there's no reason your sensitive assets shouldn't be safer this year.

Improving Wi-Fi service for a Liverpool City Centre student housing development

Lansafe Ltd installed Draytek solutions to improve the WiFi service within a Liverpool city centre student housing development.

The Requirement

- Find a reliable, low-cost Internet connectivity solution for 3 student housing buildings servicing 130+ students
- Improve the bandwidth access to the existing 4 ADSL broadbands - which were providing slow connectivity (around 15mbps) and segregated across 4 separate routers
- Improve wireless connectivity
- Cover two additional buildings for 100 students with one leased line
- Manage solution remotely

The Solution

Lansafe was contracted by a private landlord to provide Internet connectivity, residential Wi-Fi and broadband failover options for three student housing buildings located within Liverpool City Centre.

The first building housed 37 students, over 7 floors. Lansafe installed a DrayTek Vigor business class, multi-WAN router (Vigor 3320) and 2 Vigor switches (VigorSwitch P2280x) to manage primary and backup WAN connectivity to the building. The Vigor router is a quad-WAN load-balancer. The multiple WAN interfaces can be used either for WAN-Backup or Load-Balancing. WAN-Backup provides contingency (redundancy) in case of your primary ADSL line or ISP suffering temporary outage.

To offer robust Wi-Fi connectivity, Lansafe installed 8 VigorAP 912C access points throughout the building. The VigorAP 912C is a high-performance, ceiling mounted, dual-band access point. It supports up to four distinct SSIDs (for VLANs) for each frequency band within 2.4 and 5Ghz. Multiple channels were used to maximise Wi-Fi performance throughout the building.

The remaining two student housing buildings were located across the street from each other. One building housed 64 students, over 9 floors and the other building housed 35 students, over 6 floors.

Lansafe installed two Vigor 2862 routers and linked the buildings via a 1Gbps wireless point to point - linking the two sites into a primary high speed leased line Internet connection. In addition, each building was outfitted with a 24 port, PoE switch, VigorSwitch P2280x, and multiple VigorAP 912C access points.

"Within this student housing development, we have 100+ students using well in excess of 1TB of data every week – so far, the DrayTek Vigor routers have never needed to be rebooted. DrayTek solutions reinforce Lansafe's brand of being a premier provider of reliable Managed IT & Network technology solutions."

Adam Baxendale, sales director, Lansafe Ltd

An additional ADSL broadband is linked to the Vigor 2862 router in the 3rd building. This is used for VigorACS device management and broadband failover.

VigorACS is DrayTek's Central Management System (CMS). It supports all current DrayTek routers, switches and access points - providing System Integrators or system administration personnel a real-time integrated monitoring, configuration and management platform. At a glance, Lansafe can see the status and activity of DrayTek devices anywhere on the Internet, as well as receive alerts if a device has gone offline or any other alarm conditions selected.

"Our brand is all about reliable technology and IT services for small and medium sized business, education and hospitality companies in the North West of England. Our goal is to install and never receive technical fault complaints," stated Adam Baxendale, Lansafe Ltd, Sales Director.

"Within this student housing development, we have 100+ students using well in excess of 1TB of data every week – so far, the DrayTek Vigor routers have never needed to be rebooted.

Draytek Solutions reinforce Lansafe brand of being a premier provider of reliable Managed IT & Network technology solutions."

For more information, please contact:

UK/IRE Sales Contact:
info@draytek.co.uk

Main Tel: 0345 5570007
Website: www.draytek.co.uk

Production scale in IoT deployments

Nick Sacke, head of IoT and products, Comms365

IoT production deployments are underpinned by a carefully orchestrated connectivity layer, but as Nick Sacke, head of IoT and products at Comms365 explains, there are numerous key considerations that must be asked ahead of an IoT production rollout, rather than looking for a 'one size fits all' connectivity approach.

Why are there different IoT networks and protocols?

Doubt and fragmentation in the IoT market, combined with increasing software innovation, have led to the creation of several network connectivity options, each with their own attributes. We are very much still in the early adopter stage as multiple standards compete in a land-grab operation until certain standards take hold.

In recent years we've witnessed the growing expansion and evolution of the Low Power Wide Area Network (LPWAN). The early entrants to this market, LoRaWAN and Sigfox, use free-to-air radio spectrum, and have had time to establish themselves across the world. LoRaWAN, in particular, has dominated the market with over 40% market share of new connections, which is projected to continue adding market share through 2025. Both LoRaWAN and Sigfox are now acknowledged as global network and protocol standards for IoT through establishing trust with users who are confident in the usability, and reliability of such networks.

On the cellular side, for new IoT network protocols NB-IoT and LTE-M, there is still an element of catchup in progress. Despite initial predictions claiming that the cellular IoT Network variants would dominate the IoT connectivity market and squeeze LoRaWAN and Sigfox to the margins, there has been a lack of intensity in UK rollout of the cellular IoT network programmes. This means that IoT cellular LPWAN work has been largely limited to testing in the UK.

Which network type or protocol?

As with most projects, cost of delivery for data is a primary concern that must be addressed. LoRaWAN and Sigfox are now at a level of maturity where the devices are cost-effective. Initially, cellular was a much higher cost, but is now starting to achieve cost-effectiveness. But in terms of usage costs, for NB-IoT and LTE-M, users are still paying for data usage on the network, whereas LoRaWAN charges are based on device licensing, and for Sigfox, per message.

Even though there appears to be a clear differential in terms of cost models, the choice of network isn't straightforward. As IoT rollouts become more commonplace, there are elements within a LoRaWAN environment that create cause for concern. With multiple devices sharing the LoRaWAN spectrum, this can cause potential collisions on the network. In order to ensure each message arrives at its destination, the software controlling the network has been adapted further to mitigate against this happening by spreading messages across multiple channels, monitoring message counters.

Use cases

We're seeing an uptake in LoRaWAN for local governments that see it as a mechanism to scale multiple use cases at once. Additionally, in the utility monitoring sector, NB-IoT appears to be the protocol gaining the advantage, as it has deep penetration under the ground with good signal strength to reach its destination.

But when it comes to monitoring elements deep within buildings, LoRaWAN can be more effective. Refrigeration and temperature monitoring is one such example with the rollout of the Covid-19 vaccine which must be stored at precise chilled temperatures. LoRaWAN can provide an effective protocol in this instance, measuring the temperature deep inside the building, all the way down to the probe.

Blended connectivity

At this point in time, there is no one protocol that is optimised for every use case. The solution is to deploy a hybrid model, one which blends different connectivity protocols together to achieve total estate and use case coverage. A blended approach is flexible, cost-effective and scalable – ideal for those that are looking to reap the benefits of mass-scale IoT but are uncertain where to proceed.

Futureproof

Longevity is crucial for the success of an IoT deployment. No business wants to rip and replace technology after ten years. It's clear that LoRaWAN is on a growth trajectory that will provide that longevity. And the eventual maturity of 5G will also become another option for IoT projects, with much more efficiency in terms of capability to connect millions of sensors.

With a blended model of different protocols covering each estate, to make it efficient and streamlined, it's important for a single platform to be used that can bring it all together and be received and analysed in one place. NB-IoT, LoRaWAN, LTE-M, Sigfox are all becoming industry-standard protocols that are each received in a different format. But they can be streamlined into one hub that intercepts the traffic and converts it into a protocol that the receiving application requires. By working with a partner offering all types of IoT connectivity in a blended solution, projects can be rolled out in the confidence that each protocol is supported, to maximise the functionality and practicality of an entire IoT project.

Register for Networking+

The future of fibre

Fibre broadband is the backbone of UK internet infrastructure, but with the investment in new technologies, will it be as important come 2030? Robert Shepherd does some digging

Cast your mind back to the 2019 general election campaign by the Labour Party, in which then leader Jeremy Corbyn made an audacious pledge to give every home and business in the UK free full-fibre broadband by 2030 if it formed a government.

Labour suffered a thrashing at the polls and so Corbyn was unable to deliver on his promise, yet there were many detractors who saw the plan as a complete waste of money, claiming that this high-speed service could be obsolete by the end of the decade. Yet, from an enterprise's point of view, would they have been sold a dummy?

Oliver Helm, chief executive officer at Full Fibre, which provides broadband, in cities, towns, villages, businesses and homes, has a slightly different view.

"Just as the public switched telephone network (PSTN) evolved and increased bandwidth over the years, fibre has a long roadmap ahead of it," he says. "With ongoing development, it will far surpass its current capabilities – into the terabits per second - as we uncover new technologies to find fibre's full potential and fibre will be the future-proof backbone of connectivity for decades to come. It's currently the only solution that can deliver the stability and robustness required both now and far into the future, so we believe it is very much here to stay and will support our ever-growing need for robust communications."

There's no doubt that fibre is helping to future-proof the UK infrastructure, but with 5G getting stronger all the time, shouldn't we be investing more in that or wireless technology in general?

"5G and fibre can be considered complimentary technologies for a connected society," Stéphane Chabot, vice president, test and measurement at Exfo. "5G brings higher capacity, closer, to more users, but the increased density of access points in 5G means that fibre will be an absolute necessity for metro and wide area backhaul connectivity. As an example, the recent announcement from O2, Three and Vodafone to share infrastructure in pursuit of greater rural telecoms service access demands it."

Helm broadly agrees: "Wireless (whether we're talking 5G or satellite access such as SpaceX's Starlink strategy) are great solutions for specific needs, but they still need to get their bandwidth from somewhere on the ground. A growing number of homes and businesses are relying on stable, reliable, high-bandwidth fibre connections right now, and this is only going to increase as we add more smart devices to our homes and businesses."

Let's talk 5G for a moment. In terms of bandwidth, it provides around 1GB, whereas fibre can deliver up to 1TB. Yet, Farnan argues there are many specific use cases, particularly in the IoT space – smart factories, driverless vehicles, remote surgery, agriculture etc. – where 5G is providing the mobile connectivity required that fibre cannot.

"When it comes to latency, certain millimetre wave radio technologies perform better than fibre but fall short in distance," he says. "There's some interesting research going on at the moment around hollow fibre. Currently the speed of transmission in fibre is about two thirds the speed of light. In hollow fibre, the lack of glass allows speeds that near on the speed of light. Again, this is very limited in achievable distance, but it will be interesting to see possible use cases develop focused on the last mile, where you can achieve much better latency than with glass-based fibre."

Investment is clearly needed in fibre regardless, because without it there is no 5G, as the latter's success relies on a backhaul network connection that's readily available and as fast and reliable as the mobile technology itself.

Robin Farnan, executive vice president – operations and engineering, Colt Technology Services, provider of global network and voice services, says standard network architectures aren't built very well for the mobile and wireless applications of the future, where processing takes place closer to the network edge and where networks can be provisioned to deal with specific applications. "5G use cases; smart factories, hospitals, vehicles, infrastructure, etc., require high speed, reliable connectivity along with connections to key data centres," adds Farnan. "Future smart cities will be built on the foundations of a dense and wide-reaching network of high bandwidth, low latency connectivity."

Let's not forget satellite broadband, either. Farnan says suburban or rural connectivity are typical use cases, and some corporations in remote locations have been using satellites for many years. "But, yet again, this is a complementary technology rather than a threat to fibre," he says. "We can find great value in emerging technologies when we consider their unique use cases and the opportunities they provide, but I don't think they will ever be a primary technology for communications."

So, now we know how important fibre is, why is it and why should it remain the best option for enterprises?

There are of course other services and technologies out there but Helm agues the fact fibre is future-proof and highly scalable means it ensures the end-user's capacity can be simply turned up or down depending on the company's need, without new lines or downtime.

"Fully monitored end-to-end, it's reliable and low latency, which bridges the global communication divide despite the distance," he says. "It's inherently more secure and also removes the necessity for onsite servers as data can be immediately accessed remotely, allowing users to work from wherever they may be. As our technology becomes smarter fibre has the capacity and capability to enable the move to a fully connected global network with high bandwidth and minimal latency - that's why it's ideal for enterprise."

For Chabot "fibre has long been the backbone of the enterprise and will continue to dominate deployments", as more devices are connected and higher speeds are required.

"Enterprises are also faced with connecting people to applications which could be hosted on, or off premises in public, private or hybrid clouds, depending on data needs such as security, latency and processing power," Chabot continues. "High capacity, high quality, fully assured fibre data networks are going to be absolutely critical for connectivity to those cloud-centric services."

While the benefits of fibre far outweigh the negatives, the physical materials are not immune to wear and tear or unexpected damage. After all, fibre is thinner and lighter than metallic wiring, so it makes for a more delicate system. Just how problematic is that?

"True, fibre is more delicate, but it's already used in almost any imaginable environment around the world because manufacturers are offsetting these weaknesses with robust encasements that suit the environment in question," says Helm. "Our understanding of materials has evolved over the years, enabling fibre to be used in environments and conditions that were never possible with metallic wiring. It all boils down to ensuring that the glass filament is protected, and in many cases, has been given more thought and design than its metallic predecessor. However, engineers should still take care because at the end of the day, the strongest cable – metallic or fibre - can still be damaged by sub-standard installation."

"When it comes to latency, certain millimetre wave radio technologies perform better than fibre but fall short in distance"

Robin Farnan, executive vice president – operations and engineering, Colt Technology Services

Then, of course, there's 'fibre use', which is a catastrophic effect that occurs when an imperfection in the fibre precipitates heating and the local temperature approaches 1000 °C. At that elevated temperature, laser radiation propagating through the fibre is strongly absorbed, resulting in the temperature escalating rapidly. Surely, that's also a major concern?

Helm argues that "as with any technology, if you purchase poorly manufactured products", installation standards are not high enough, or usage exceeds the product's capability, there is going to be a failure at some point – it's a given, the question then becomes 'when?'

He continues: "Fibre fuse can affect large lengths of fibre, even kilometre's-worth of infrastructure, but one of the major benefits of fibre is that everything can be proactively monitored at both ends. Meaning imperfections and capacity issues can be immediately reported as soon as they appear, reducing the chances of an outage and negating much of that risk."

Great, then, that there are procedures in place to help prolong the life of fibre kit, but just how often does it need to be updated? Or, in other words, how sustainable is it?

"It is more than sustainable, says Chabot. "Fibres are engineered for 25-30+ years. It is the cables themselves (shielding the fibres) that have a shorter lifespan, where the physical longevity of the cable will range from 20-25 years.

Farnan concurs and adds that laying new fibre leaves a carbon footprint; the process of creating the physical fibre and the process of physically digging and laying that fibre in the ground both incur environmental costs. "Technology and processes can help make fibre more sustainable and there's a lot of effort going into this area," adds Farnan. "There are technologies that increase fibre capacity and provide more bandwidth for the same amount of fibre; increasing efficiency and avoiding the need to lay new."

Colt, Farnan says, uses AI to mine our inventory systems to identify ceased fibre that we can reuse elsewhere; saving on new fibre, its related digging and the carbon emissions involved.

Another accusation levelled at fibre is that cables are limited in the sense that they can only propagate light in one direction. If bidirectional communication is necessary, does mean extra costs?

"Not necessarily," says Helm. "It is more about the transceivers at either end of the fibre than the fibre cable itself. Right now, the cost-effective method is to leverage two cables, one in either direction, which is why we see many fibre providers offering synchronous services, which was not the norm with traditional copper technologies. But bidirectional transmission over a single filament is possible, using different wavelengths for each direction, which is where a lot of the research and development in fibre is currently focussed. If we can find ways to layer even more wavelengths, then the possible potential for fibre grows dramatically and we're excited to see where this may lead."

Then, of course, there's expense. Offering the best technology and service is one thing, but what's being done to bring down the cost of fibre?

Helm says just like any other product, price fluctuates through supply and demand, exchange rates, manufacturing costs, etc. "Fibre is now manufactured around the world, has a good level of competitors that is constantly growing. Early patents are coming to a close and it is now a very much established and tested product, so prices are falling," he continues. "But as our understanding of the material and data processing in general advances, manufacturing costs will continue to drop, reliability will increase and competition will grow, driving down long-term costs even further for the supply chain."

Chabot argues that there will always be competing technologies, such as the emergence of a new generation of high-capacity satellite systems and private wireless networks. "Ultimately, enterprises will choose whichever connectivity solution suits them best," he says. "However, fibre is a proven technology offering an ultra-reliable high-speed connection, which is still undergoing its own evolution in capabilities, often itself "back hauling" private wireless and satellite access points to data centres.

Farnan believes not only that fibre will still be around at the turn of the decade, it will be everywhere.

There are signs of this in the many rollout initiatives seen across the world, in particular around FFTx in all countries, as well as government-funded projects," he says. "In 10 years' time, I think this acceleration of fibre availability will have reached far and wide, missing out only the most rural areas."

However, Farnan says the threat to fibre is that it will become a commodity and that its value will be eroded over time. That's why operators like Colt are also investing in the overlay and focusing on the service layer as a differentiator," he adds. "Eventually there will be more opportunity found in partnering with other operators to gain complementary coverage than in digging new. There's no point in spending huge amounts of money laying your own fibre when fibre is already there, ready to be used in an ecosystem collaboration with a partner."

That said, fibre sounds like it has a safe future…for now at least.

"Looking at bandwidth capacity, there is nothing that can surpass fibre today and in the near term," concludes Farnan. "But emerging technologies have a role to play and there are some use cases fibre cannot cover." Time will tell. ■

sepura

Sepura TETRA Radios

Chosen by the Metropolitan Police Service to power their next generation communications.

To find out why, visit **sepura.com**

It's all just data over the bridge

The six-month adequacy bridge was introduced to maintain the status quo for data movement between the UK and EU, but what happens after that? Robert Shepherd asks the questions

As 2020 came to a close, the United Kingdom (UK) and the European Union (EU) thrashed out a deal – as part of the long-drawn-out Brexit negotiations – to facilitate the movement and security of data between the exiting country and the 27-member bloc. Well, they agreed to a deal under which the EU will continue to treat the UK as an adequate jurisdiction for up to six months pending any full adequacy finding for the UK. This means that, for now, personal data can continue to flow from the EU to the UK without the need for millions of contracts and impact assessments. Does that mean that there is no change on the privacy front post-Brexit? Not quite.

There was some positive news last weekend when the European Commission (EC) – yes, the one the UK had a public spat with over the Covid-19 vaccine roll out - confirmed it had kick-started a process that will enable the personal data of EU citizens to be sent freely to these shores. All being well, it will save businesses on both sides of la Manche billions of pounds and euros in the process. However, it's too early to start popping the champagne corks just yet as there is still much to be done and there's no guarantee what will happen when the honeymoon period is over.

"The interim period is four months but will automatically be extended for a further two months if an agreement is not met," says Neil Thacker, DPO and CISO for security specialist Netskope. After the full six months, there are two options: the EU will either adopt an adequacy decision for the UK, or the UK will amend the UK GDPR or UK Data Protection Act 2018 without the consent of the EU, which will automatically end the temporary agreement."

Upon the expiry of the interim period, the UK will then default to a 'third country' under the GDPR with all its consequences. Reinout Bautz, general counsel at European outbound email security specialist, Zivver, says additional measures need to be invoked. "For example, the existing data processing agreements with external parties will no longer be sufficient and another 'standard' agreement with all such controllers / processors / sub-processors would need to be executed," he continues.

Zivver boasts a list of clients consisting of UK mortgage lender Paratus AMC, Douglas Macmillan Hospice, Fetal Medicine and the Dutch Judicial System. Zivver says companies in these sectors are specifically interested in its solution to help them secure outbound email communications and ensure compliance with evolving data protection regulations.

Bautz adds that when a company is part of a group of companies in Europe, the internal transfer of personal data also needs to be accommodated. "A party may consider for this preparing Binding Corporate Rules, as described in the GDPR," he continues. "However, this is a very burdensome and time-consuming exercise and has to be approved by a leading supervisory body within the EU. Given the current workload of all such supervisory bodies, it is unlikely that this could be arranged quickly."

Indeed, Heimdal Security, a Danish cybersecurity specialist headquartered in Copenhagen, is taking the bold move to build a strong presence in the UK despite Brexit. What's more, Ruth Schofield, the firm's UK country manager, says our enterprises should "absolutely" be worried about security when the data adequacy bridge deal comes to an end.

"We firmly do believe that when a deal eventually expires, even after a possible extension, this will have a strong impact on the flow of data between the UK and the EU, especially where data is put 'at rest', warns Schofield. "The problem applies to both the EU and the UK. The UK has a very strong spending on cybersecurity posture and better than EU average, but the EU has a very firm belief in enforcing its GDPR principles. If those principles are compromised will be tough to accept for EU politicians and hence a likely battle between the EU and the UK is on the horizon, as to where and how data is put at rest."

Register for Networking+

Meanwhile, Sophie Chase-Borthwick, VP of data ethics and privacy at end-to-end managed data services provider, Calligo, warns that "without trying to cause alarm, there is no sign yet that adequacy will be awarded to the UK", which means we don't know exactly how things will look like at the end of the bridge period. What's more, she adds that awarding adequacy takes time – to date, the quickest it has been awarded was in the case of Argentina and that took some 18 months to happen.

That said, it appears the UK might not have an uphill task to get what it needs.

"In some ways, the UK is well placed to be awarded adequacy," Chase-Borthwick argues. "The UK's Data Protection Act 2018 was arguably written as an implementing act of GDPR aligning with EU regulations. However, there are some misalignments with the UK's Investigative Powers Act 2016, and the Data Protection Act and the EU's Charter of Fundamental Rights. In addition, the UK's close security relationship with Australia may also come under the spotlight. Australia was itself refused adequacy by the EU."

She adds that "with that in mind", even an ex-EU member cannot take achieving adequacy as a mere formality. If it's not confirmed by June 30, 2021, or there is no further extension, data transfers will default to being at risk of being instantly prohibited. "Any business with operations in the UK that processes EU personal data will therefore need to adapt its own data strategies to provide the necessary protections that the EU requires and that the UK's national legislation would technically have been deemed to not require," says Chase-Borthwick.

With no definite measures in place, UK enterprises will be venturing into the unknown – does that mean they will be more exposed to hacking?

"Yes, but as UK businesses in many cases already have a solid spend on cybersecurity, we firmly believe that the only change required is towards more innovative and ground-breaking solutions, where the mobility of the data and the user is taken into consideration," says Schofield. "We see the UK companies spending is still being more around reactive security posture spending, such as antivirus and detection, whereas EU companies are leaning more towards mitigating excessive user rights or other problems before they escalate, and by auditing threats before they are allowed to enter the company domain."

So, if things are likely to get worse before they get better, what's the thinking behind opening a UK presence at what is arguably the worst time to do so?

"The UK is a critical region for Heimdal's global growth strategy," Schofield continues. "We envisage the challenges of data security/data protection heightening further with post Brexit panic potentially exacerbating those challenges. Equally UK industry will benefit hugely from Heimdal's mitigative approach to securing their data and fundamentally how we provision this is in full accordance with GDPR."

Now, it's time to look at the options open to enterprises – in other words, how can they protect themselves?

"There are some measures that companies ought to be taking urgently simply because the UK has left the EU, and regardless of any adequacy decision," says Chase-Borthwick. "These are: whether they need to update privacy notices, whether they need to add a new lead supervisory authority or amend the current one. For a business that targets the EU market, they might need to appoint an EU Representative within the EEA to act as a local point of contact for individuals and EEA data protection authorities."

That's not all. Chase-Borthwick says firms must also consider what mechanisms they use to legally transfer personal data between the UK, EEA countries and non-EEA countries, and whether these are suitable in light of the Schrems II decision.

"In addition, if adequacy is not granted, businesses then have further obligations," she continues. "If a business transfers personal data from EEA into the UK it must ensure appropriate safeguards are in place, as per Article 46 of the GDPR. These include: standard contractual clauses, binding corporate rules (rarely used and require supervisory authority approval) derogations and specific data subject consent. Plus, if they are transferring personal data that is subject to the GDPR from outside the EEA into the UK (i.e. non-EEA to non-EEA) technically, they may only rely on consent or binding corporate rules. However, it is generally accepted that where these are not feasible, standard contractual clauses are unlikely to be challenged."

Scaremongering stories will abound, but Bautz says that while it is not "it is not anticipated that the agreement will expire without a further arrangement in place, an extension (or a superseding adequacy decision) is the most likely outcome".

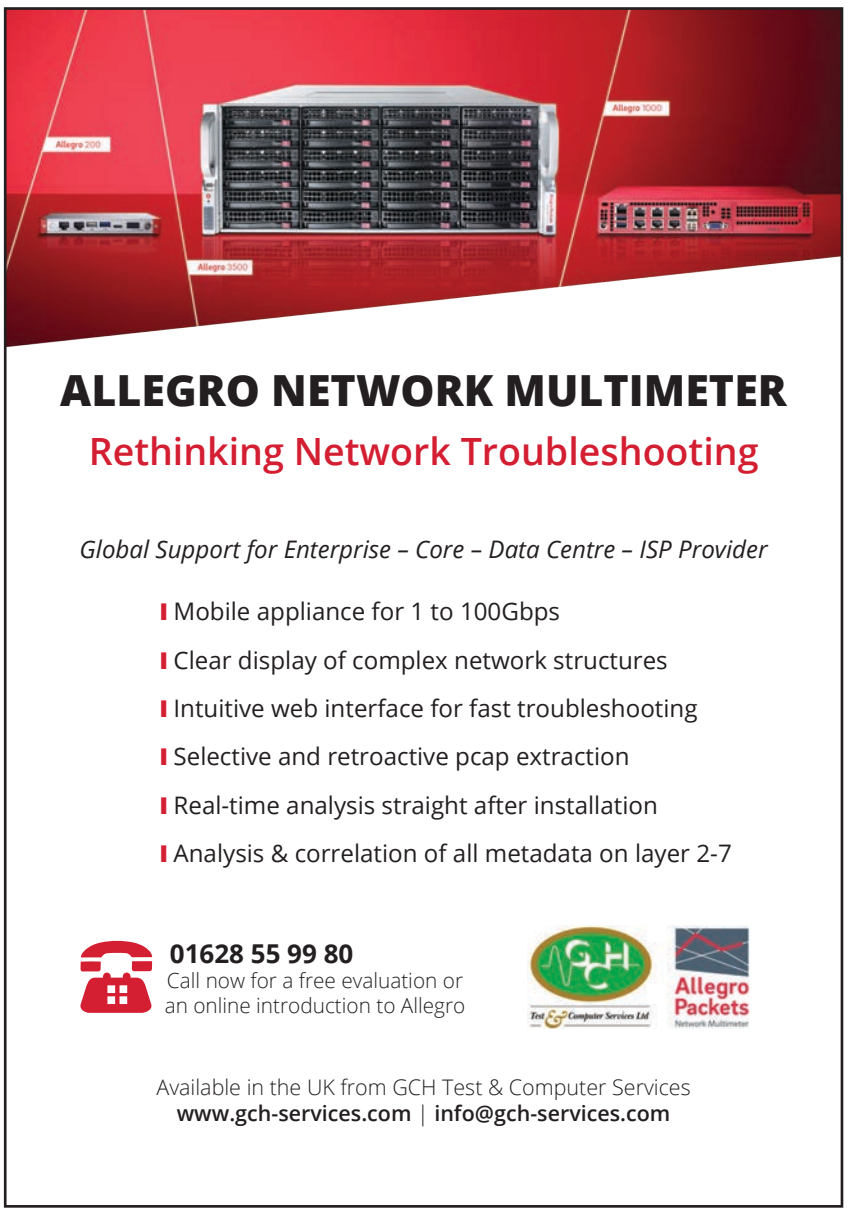
Thacker is of a similar opinion and warns that for the benefit of citizens and businesses, both the EU and UK will want to come to an agreement within the six months. "As we have seen during previous negotiations, delays and uncertainty directly impact businesses," he continues. "Enterprises should already have a good understanding of data flows from the EU to the UK and vice-versa as well as data flows across the globe. This is currently a legal requirement under General Data Protection Regulation (GDPR) whereby organisations must have an accurate and up-to-date Record of Processing Activities (RoPA - see Article 30). This RoPA should include details of where the data resides and what data transfer agreement is in place to allow for the data to be transferred."

Thacker further argues that "it is imperative that organisations keep this record up-to-date and include all details of data transfers", including any cloud service providers that are used.

"As the average enterprise organisation uses over 1000+ cloud services, it becomes a fundamental requirement that they continually assess any new cloud services that are introduced," he adds. "For all UK-EU and EU-UK transfers, organisations should be prepared to include Standard Contractual Clauses (SCCs) as an alternative to an adequacy agreement."

Businesses in all sectors must take notice of this agreement, says Thacker, as any industry that relies on the free flow of data between EU-UK and vice versa could be impacted. Bautz says there are some sectors that might be more worried than others. "Those [sectors] that process a lot of personal data, including - but not limited to - financial services, legal, healthcare and other parts of the public sector," he says. "As for such sectors, potentially many data processing agreements and internal data transfer arrangements are in place and have to be reviewed."

The movement of data is only going to get faster, so businesses will be hoping a decision will be made just as quickly. ■



Data privacy impact in the digital era

Zack Zilakakis, product evangelist, Juniper Networks

Data privacy and protection is top of mind for many organisations. Europe's tough standards could influence the future of data privacy and protection standards, writes Zack Zilakakis, product evangelist at Juniper Networks.

Organisations are increasingly concerned over their data privacy and protection strategies. Top of the heap of concerns is how the different types of regulation facing each organisation will impact their public cloud initiatives. There are potentially dozens of regulations, between the various industries and countries, requiring compliance.

The second issue is that your company is ultimately responsible for its operations. Public clouds like AWS function on a shared responsibility model when it comes to compliance. While AWS is responsible for items such as physical security and data centre operations, the customer (in other words you) are responsible for properly securing virtual networks and Amazon EC2 instances running within AWS. The compliance certifications achieved by AWS only cover its portion of the shared responsibility model. This is crucial to remember when considering your risk profile.

When it comes to protecting data, Europe's General Data Protection Regulation (GDPR) is top of mind for many. As if GDPR didn't represent enough of a compliance headache already, there is much uncertainty around what will happen in the wake of the UK leaving the EU. And there is ongoing controversy about whether GDPR places a disproportionate burden on smaller organisations.

And GDPR is, by no means, the only regulatory game in town. The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California. Similar in certain respects to GDPR, it has the important distinction of being focused around consumers of data more than data itself. And there's a variety of industries, such as health care, defense, finance, and insurance are highly regulated, and companies in these industries must comply with different regulations handed down by governing bodies.

A variety of regulations create a direct responsibility for companies to be good stewards of their customers' information, and different industries are beholden to specific regulations governing the handling of data, enforcement of security, and adherence to proper processes and procedures. Several examples include:

- Health Insurance Portability and Accountability Act (HIPAA), which stipulates how patient data must be handled through its lifecycle in the healthcare industry.
- The Federal Risk and Authorization Management Program (FedRAMP) or the Defense Acquisition Regulations System (DFARS) for defense contractors.
- The North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) for power generation and distribution.

AWS security, compliance, and data sovereignty

Compliance with regulations is the responsibility of the company, which is ultimately held accountable for violations—even if the violation was committed by a third-party, such as a public cloud provider.

Cloud providers are not able to provide the necessary compliance. Companies must pursue alternatives to cloud providers in order to meet their specific regulatory compliance requirements. ESG predicts that nearly nine of ten organizations expect most (35%) or at least half (54%) of their applications/workloads to be running on-premises in three years.

In addition to what data is stored and how it is stored, countries are becoming increasingly concerned about where the data generated by their citizens is stored. In some cases, they've enacted rules that prevent the storage of information about their citizens outside of sovereign soil. Germany's privacy laws require that storage of data about German citizens reside on servers physically located in Germany. To meet the demands of Germany and other countries like France, Russia, and China, cloud providers and companies are being forced to establish a physical presence in those countries.

Industries like finance, insurance and health care are heavily regulated and subject to strict compliance policies. These make moving workloads and data to the cloud challenging, not least because of the loss of local control they represent for admins. And while cloud companies continue to evolve, its current security and compliance offerings do not yet satisfy these regulated industries in which data privacy is held to the strictest requirements.

It used to be said that 'cash is king', but today 'data is king'. Such is the level of scrutiny around the handling of that data, far tighter than surrounds the handling of cash, no organization should face the challenge alone. With the right partner and the right tools, a complex mesh of interconnected problems can be mitigated.

The issue of data privacy and cloud is not standing still, with new regulations continually in the pipeline. The way in which organisations use and rely on the cloud is also a moveable feast. Nobody anticipated the rush to embrace remote working that we saw in 2020, and the impact that had on cloud migration strategies and data security policies. Strategies on everything from business continuity to digital transformation are being rethought as everybody adjusts to the 'new normal' and prepares for possible future disruption. Data, and the security of data, is central to all plans.

Register for Networking+

Creating a secure Internet of Things backbone for industry 4.0

As cyber-attacks become more sophisticated, how can organisations stay protected? Martin Blunn from Solutionize Global provides this insight

It's not an over-exaggeration to say that the Internet of Things (IoT) is going to have a huge impact on global technology usage throughout the coming years.

According to the Ericsson IoT forecast report, it's predicted there will be around 29 billion connected devices by 2022 – 18 billion of which will be IoT-related.

And, although the technology and adoption itself are still relatively in their infancy, organisations are becoming more acutely aware of the opportunity that IoT presents as enterprises gain a fuller understanding of what may lie ahead for the tech industry – and the variety of use cases that IoT connected devices can positively impact.

Delving further into industry research that is currently supporting evidence around IoT's early impact, Vodafone's sixth IoT Barometer document reveals that 34% of businesses surveyed in 2019 were using IoT services. And, 84% of those adopters have increased confidence in the systems compared to 12 months ago, as a result.

Perhaps more importantly too, is that 76% of the enterprises surveyed currently utilising IoT believe it is 'mission critical' for their organisations.

Further statistics go a significant distance to back up this tech evolution too, with 74% of organisations believing that the companies unable to become IoT-agile will fall behind their competitors – in only five years' time.

So, with Industry 4.0 in full throttle, can firms truly afford to ignore IoT's potential to dominate the tech sector? And do they fully understand exactly what that means?

Firstly, there are a number of elements that need to be addressed, in order for a firm to become IoT ready – and there's nothing more important than security.

As any industry knows, online protection is of paramount importance and data breaches can seriously damage a business, placing its entire future in doubt. In the case of Industrial IoT, a breach could quite literally cause a national emergency.

Savvy organisations recognise that whilst IoT presents a vast array of opportunities there are also challenges too – if a business isn't fully prepared. Why? Because, simply put, they're opening up a suite of devices that are all connected to the internet.

So, how do they know that every piece of tech is robust and business-safe from a serious cyber-attack?

A range of options to consider

There are many ways in which firms can ensure security is at the forefront of their mind – as long as they have key technologies in place. A few recommendations include Message Query Telemetry Transport (MQTT) – which is available in a number of varieties, including open source such as Mosquitto. Additionally, having separate key pairs for each IoT device and a secure boot is vital. They must also ensure compatibility with both Narrow Band IoT and Long-Term Evolution mobile networks.

Enterprises should be perfectly positioned to understand how an IoT device provides a source of continuous telemetry which – depending on the device – can be small and infrequent, to diverse and at a high frequency. Depending on the sensitive nature of this telemetry feed, transmission needs to be secured from the point of transmission to the consumption of the data.

There is a minimum level of security for businesses via TLS's most recent version too, alongside the use of a certificate authority – whether this is contained within the organisation or by a public issuing body. However, if it requires further secure communication methods, it's recommended to go with a VPN solution.

Additionally, companies exploring 'Defence in Depth' (DiD) security enables them to further safeguard their connected devices, ensuring they're not vulnerable to IoT attacks. How this works is through a robust approach to cybersecurity in which a series of defensive mechanisms are layered – meaning every phase is protecting valuable data and information.

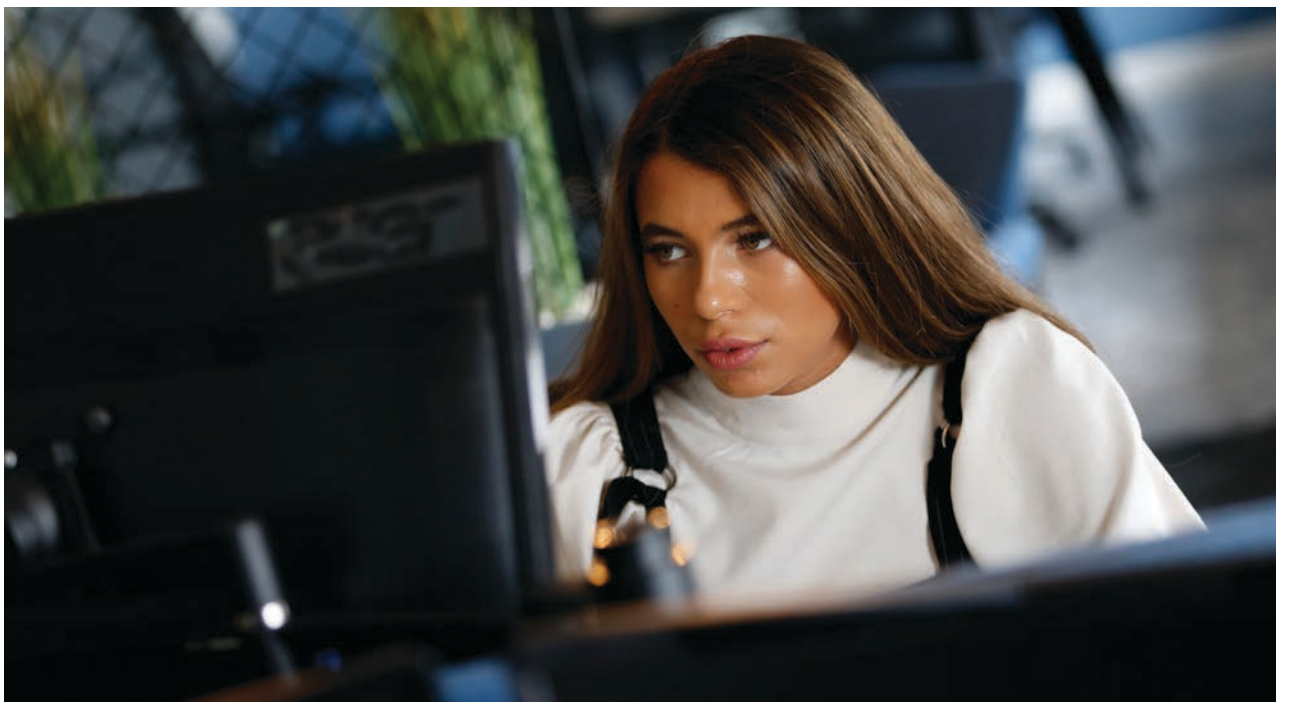
Is the firm IoT secure and ready?

There are a number of options for organisations to consider – all of which can be explained in detail by a managed services provider should that be the route the business wants to take.

IoT presents many benefits for enterprises – from enhancing productivity to making operations more streamlined. It's important for entities to assess the range of options available when it comes to ensuring their suite of devices are securely protected and secure from attack.

However, companies should never rest when it comes to safety and must always make sure they're up to speed with the type of security they need – even when using IoT services on a subscription basis.

If it's handled correctly, and a firm is robustly protected, organisations can not only be equipped with the correct level of security, but also provide further trust and support for the customer they serve. From regularly undertaking the basics – such as relatively simple tasks including resetting passwords, locking smartphones, deploying end-to-end encryption and updating firmware as often as is needed – IoT should be welcomed by modern-day firms for the true benefits it can provide, not feared. ■



IoT presents many benefits for enterprises – from enhancing productivity to making operations more streamlined. It's important for entities to assess the range of options available when it comes to ensuring their suite of devices are securely protected and secure from attack

UC solutions and top tips

David Samuel, managing director at 24 Seven Cloud

In these times of extreme uncertainty, choosing a UC solution which will work with your existing hardware is a way of 'upcycling' your existing phone system & adding 21st Century solutions such as video conferencing, easy home-working and collaboration without any CAPEX costs. You should also ensure that any UC solution you are considering will be compatible with your business' future plans so that you don't end up having to get rid of the solution you implemented during lockdown when everyone is back in the office. Look for solutions which offer easy CRM integration, Call Centre and Call reporting options, business-grade call-recording solutions as well as integrations with technologies which businesses have relied on during lockdown such as Microsoft Teams.

Communication & collaboration in one place

The best UC solutions are a phone, a personal assistant and a complete business solution – all wrapped into one. Therefore, look for an innovative platform where you can access all of your messages, calls and contacts to ensure that collaboration and communication levels are never compromised. From long video conferences to quick-fire instant messages, you can have a wide range of features and functionalities at your fingertips to help bolster your business operations. Having them all in one place, on one platform is a huge benefit.

Work from anywhere!

In the world of change we find ourselves in, look for a solution that works on multiple devices. You no longer 'have to be' in the office, or at your desk to receive a call, join a meeting or access certain information. Unified Communications also unifies all your devices so you can receive/make calls on your desk phone, mobile, PC, even a tablet.

Secure and easy to manage portal

Another factor to look for is an easy to manage portal, the functionalities and capabilities that you can perform yourself, without going through a third party are staggering. Whether you are looking to simply communicate with your team or manage your overall business' telecoms system – you can do it all yourself.

Packages

Look out for solutions that offer a variety of packages, tiered with different feature and functionality offerings. That way, you don't have to overpay for features that you'd never use and waste your money. The best will offer packages suitable for all businesses – no matter what size or industry. Check out upgrade availability too so your solution can grow as your business does. Nowadays you also don't have to sign up to long lengthy contracts.

CRM Integration

The customer experience has to be at the forefront of all businesses, especially at the moment. If a customer calls and no one answers, they could very well think that business is not currently operating and move over to a competitor. The same could be said for all your colleagues working from home. To have information on all customers up front will make all the difference. It is imperative therefore to use a UC solution that links seamlessly with your CRM platform. This will drive efficiency across your business.

Costs

In 2025, BT are switching off all analogue lines so finding the perfect cloud-based solution now is a sure way of future-proofing your business Cloud-based phone systems are a lot cheaper than traditional ones, as you don't have all the hardware and software to purchase. You only have to pay a monthly fee for your seat and the internet that you use. So, you can kiss goodbye to hefty bills at the end of the month and be able to forecast your outgoings a lot more accurately.

Security & Resilience

This time last year not many of us had heard of Zoom, but it is now a household name for all ages! They have clearly stormed the 'video-meeting' market, however even they have had some bad press and security issues. Whichever company you go with ensure that their solution is fully secure with the correct firewalls in place. Also check their uptime and resilience. Once you have all your communications unified, you don't want the system to keep crashing!

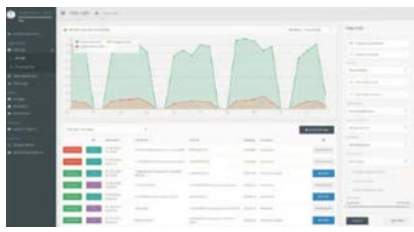
Additional services

As with a lot of things it is often best to use one supplier for different services. That way you only have one port of call, and the services work in conjunction with each other. Additional services can include call recording, contact centre solutions, call reporting, auto attendants even hardware solutions.

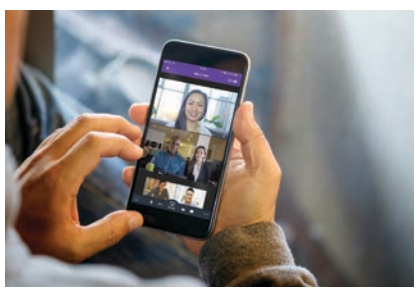
PRODUCTS

Giacom is focused on the software distribution sector through its online cloud marketplace. Communication is essential, more so than ever now with social distancing measures in place and remote working an essential tool for many businesses – it shouldn't be an additional challenge for businesses trying to survive. The channel-only cloud services provider offers a variety of unified communications products for ITCs to provision for end users, including Microsoft Teams and Business Voice. Built into Microsoft 365, Microsoft Teams is a hub for teamwork, combining chat, calling and document collaboration in a single, integrated app. It's a complete solution for effective collaboration and communication, which is key during challenging times while workforces are dispersed. Microsoft Teams enables users to integrate scheduling, note-taking and desktop sharing for online meetings, irrespective of location, helping to keep everyone in the business on the same page. With this unified chat-space, Giacom offers ITCs to empower their customers with the option to have complete end-to-end calling through Microsoft Business Voice, allowing them to have full voice capability. The cloud-based small business phone system is an add-on for Microsoft 365 plans, creating a 'virtual office' by allowing businesses to connect from any device or location. The combination of unified communication products creates an all-in-one communication system, which is essential for managing remote teams in order to collaborate and communicate. Giacom also offers alternatives to ITCs, including Direct Routing, which is a cost-effective alternative to calling plans for Microsoft 365, allowing organisations to replace any existing phone system with Teams for all inbound and outbound calling to landlines and mobiles.

Many businesses are looking to equip remote workforces with cloud communications tools at the moment. Whether managing a geographically dispersed workforce or looking to move to a cloud-based work environment, many are starting to contemplate a move to all-IP telephony to increase control over cost and people efficiencies. There's also the small matter of the 2025 ISDN and PSTN switch off, which is also driving the need to change. **Clear Voice** is the new carrier-grade hosted voice platform from Vaioni Wholesale, aimed at telecoms channel partners offering 'work from anywhere' solutions to business customers. It offers unified communications features as standard, backed with comprehensive analytics. Vaioni says it's perfect for organisations looking to get better control of costs, move to a more flexible and adaptable system to accommodate change, and equip their staff for new ways of working either remotely or from the office. The platform includes a range of call management features, including automatic call recording with lifetime storage, call routing, MiFID II and PCI compliance, Hunt Groups and Wallboards. These features are all accessible through a softphone client on mobile or desktop, or more traditionally through a desktop phone. Clear Voice also integrates with Microsoft Teams. Businesses using Clear Voice can scale their service quickly and easily. Clear Voice is 100% self-service from within a single portal, making it easy to use and administer. Licenses can be added at the click of a button without the need for purchasing handsets.



Fuze is recognised for its ability to deliver a differentiated user experience for communication and collaboration on both desktop and mobile devices. The company provides an intuitive, cloud-based all-in-one unified communications as a service (UCaaS) platform for mid-market and enterprise companies. Powered by intelligent cloud architecture, Fuze combines calling, meeting, chatting, and sharing in one platform, empowering the digital workforce anytime, anywhere, and across any device. With three UCaaS product solutions – Fuze Calling, Fuze Meetings and Fuze Contact Centre – the company provides users with transition between calling, video conferencing, instant messaging, and sharing. Using a single carrier network, Fuze Calling offers a secure system beyond voice by seamlessly integrating with video and real-time content sharing on any device. Fuze Meetings provides enterprise-grade HD audio and video conferencing for up to 1,000 meeting participants and enables screen and content sharing. Fuze Contact Centre, a fully integrated contact centre as a service (CCaaS) solution provides a powerful call routing engine and ensures callers are directed to the right agent quickly, securely and with good voice quality. The suite of integrations connect to and integrate with applications such as Office 365, G Suite, Salesforce, Slack, Microsoft Teams, or Zendesk – eliminating the need to toggle between apps and Fuze.



Cinos has a strong focus within the UK public sector. Taking commercial-off-the-shelf technology from leading vendors, Cinos delivers an end-to-end service that allows customers to collaborate from any location, on any device. Cinos Cloud UC services are available over the internet, via Cinos private WAN connection and delivered natively into the Health and Social Care Network for NHS and healthcare customers. This includes SIP and PSTN connection as well as Direct Routing for Microsoft Teams to ensure secure, reliable cloud communications. When delivering voice, video or content collaboration, integration is key. From managing large multi-vendor solutions to simplifying communications with different providers and platforms. Cinos Cloud UC services interoperate with other systems to make meetings safe, simple and productive, whether that's an interactive huddle space, meeting room or large auditorium/learning space. Cinos also delivers voice and multimedia interactions to customer service teams based in contact centres. Using automation, chatbots and self-service tools, organisations are able to link interactions so they can ensure important details will follow their customers however they choose to contact them. Spanning customer premises, public, private and hybrid-cloud environments, Cinos offers an infrastructure that is deployed across geo-redundant data centres and supports workloads up to SECRET (Tier 2) Government Security Classification as well as adhering to all NCSC security principles.

Please meet...

Al Taylor, co-founder, cloudDNA

What was your big career break?

I was a late starter in the industry and met my business partner (who is now also my wife) when we both worked for an IT distributor in the late 2000s. I looked after the Citrix Networking product set (NetScaler and WANScaler at the time) and she was the Citrix Marketing Manager. She would help partners find business and I'd help them close it. After 5 years of helping others we had a 'screw it, let's do it' moment and founded cloudDNA as a centre of Citrix Networking excellence back in November 2012. We've had some tough days along the way but it's been an amazing journey so far.

Who was your hero when you were growing up?

I was born in the 70s but grew up in the 80s at a time when digital synthesizers really took off and while there were many artists and songs that caught my imagination, Jean-Michel Jarre was a real inspiration. His concerts in Houston and London completely blew my mind from the epic light shows to the instruments he played. I had no interest in reading music but could play the vast majority of things I heard 'by ear', including all of his albums on my Casio keyboard. I collected various bits of kit (synths, drum machines, effects etc) over the years and hooked them all up with MIDI which I guess was a basic introduction to the networking principles I use today.

What's the strangest thing someone has asked you to do?

Go halves on a fire engine to convert to a limo. I thought it was bonkers so didn't hesitate to get involved. It was so busy we ended up with two of them. Kids parties in the afternoons, hen parties and birthdays in the evenings. Mirror ball, massive sound system and furry seats on the inside, 100% stock Dennis fire engine on the outside. One of our drivers was coming back following a night out and was inadvertently first on the scene at a car accident at 3 am one morning. He was busy doing first aid when the real fire service turned up looking very bemused…

What would you do with £1m?

I'd sort out the fridge on our 1981 VW Camper for a start, been meaning to do that for years.

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

'Two ears, one mouth' or 'Seek first to understand, then be understood.' One is from Mrs Taylor, the other from 7 Habits of Highly Effective People by Stephen R Covey but they both effectively mean the same thing. Listen first and your discussions will be far more rewarding.

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

It's a different world now but I'd probably go back in the music industry. I found it was easier to earn a living swap synths for records and started getting paid gigs as a DJ at the back end of the 90s. I ended up on contract working for one of the big PLCs that operated the Liquid and Oceana venues up and down the country. Student nights in the week, club nights at the weekend, 5 or 6 nights a week. I was resident in a venue in Lincoln when I met a guy who went to work for Kiss FM in London. In true Dick Wittington style, I ended my contracts and moved down south, did a TV presenting course and started networking a way to get some gigs. I did corporate stuff like the De Beers (diamonds) wrap party for the filming of the Casino Royal Bond film in The Café de Paris, Empire Casino in Leicester Square and the like before being introduced to a couple of folks from Ministry of Sound and ultimately ended up DJing on global tours for a couple of their brands and working as a Production Manager for HedKandi. Fun times and only stopped on doctor's orders as I'm now officially deaf but the ear defenders are much better these days.

The Beatles or the Rolling Stones?

I'm house music through and through and wouldn't listen to either by choice. The Beatles generally sounded miserable, the Stones too shouty and those scratchy guitars play havoc with my tinnitus.

If money was no object, where would you live?

We're really fortunate to live by the Thames on the Berks/Bucks border and despite having credible opportunities to move elsewhere, it's my favourite place in the UK so can't see us moving from here any time soon. That said, I could be tempted by California. We've had some extended trips around the state to coincide with Citrix events and spent some time in LA and San Francisco which are both very different but equally appealing. We had planned to drive the coast road between the two cities this month but Covid has kiboshed that for this year.

What's the one thing you'll miss about Donald Trump?

He's not my cup of tea but he is a master at marketing his own brand. There have been a couple of recent documentaries that chart his progress from his failed business to becoming president and they are a fascinating insight on the way the modern world works.