SEPTEMBER 2021
networkingplus.co.uk

NETWORK+

Security insight

Security challenges posed managing hybrid identity environments

Sean Deuby, Semperis, p6

From survive to thrive

Unlocking RoI

Keith Ali, Creative ITC, p7

Questions & answers

'What I'd do with £1m'

Nick Dobrovolskiy, Parallels, p16

MoD apologises for Afghanistan data breach

The Ministry of Defence (MoD) has apologised following a major "data breach" that reportedly exposed the email addresses of more than 250 interpreters who remain in Afghanistan.

Defence secretary Ben Wallace said it would be an understatement to say he was angered after a number of people seeking relocation to the UK – many of whom are still hiding from the new Taliban government – were mistakenly copied into an email.

The minister has apologised to those affected and launched an investigation. One person has been suspended, he said.

Once the mistake had been made apparent, the MoD then sent another email 30 minutes later with the title "Urgent - Arap case contact" asking the recipients to delete the previous email and warning "your email address may have been compromised".

It also recommended the interpreters change their email addresses.

The MoD has also referred itself to the Information Commissioner's Office.

Addressing fellow MPs in the House of Commons, Wallace said: "I apologise to those Afghans affected by this data breach and with Home (the Home Office) we are now working with them to provide security advice. It is an unacceptable level of service that has let down the thousands of members of the armed forces and veterans. On behalf of the Ministry of Defence, I apologise."

An MoD spokesperson added that an investigation has been launched into a data breach of information from the Afghan Relocations Assistance Policy team.

"We apologise to everyone impacted by this breach and are working hard to ensure it does not happen again," the spokesperson added. "The Ministry of Defence takes its information and data handling responsibilities very seriously."

The MoD has said it will take all necessary steps under UK GDPR (General Data Protection Regulation) rules.

Wouter Klinkhamer, chief executive officer at secure communication solutions specialist Zivver, said news of the data breach "is a stark reality" of what can happen when digital communications are not safeguarded.

"This is an extreme example of course where the data breach is potentially life-threatening; but all business leaders need to sit back and review how sensitive information is being shared and ask what support does its workforce have to communicate securely," he said. "It's common that incidents such as this are a result of human error (verified by the UK's ICO) – an employee inadvertently selecting 'Cc' instead of 'Bcc' before sending the email."

Klinkhamer added that while "we're all human, we all make mistakes" – organisations need to focus on how they can empower their individuals to be able to share information securely "when they need, with confidence and with ease to avoid a potentially damaging situation". ■

Telehouse upgrades 'most connected data centre building in Europe'

Telehouse International has upgraded its Telehouse North data centre in London, which has been carried out to support growing demand for colocation space at the facility.

The new-look centre offers additional capacity for service providers, including ISPs, ASPs and system integrators, looking to join or expand in what the company says is the most connected data centre in Europe.

This upgrade entailed a complete refurbishment of the TFM25 suite within Telehouse North, which has increased space for new and existing customers as well as power per rack from 0.5-1kW to 3kW.

Significant investment in this refurbishment project is in response to the growing demand for colocation space within Telehouse North, it said. Opening in October 2021, the newly refurbished suite will deliver higher power densities in line with modern day demands, as well as a fully redundant power supply to meet increasing resiliency requirements. Existing Telehouse North customers can now take extra capacity within this data centre while new customers can join the expanding Telehouse North carrier community.

Opened in 1990, Telehouse North was the first purpose-built colocation data centre in Europe. It has been the primary home for the London Internet Exchange (LINX) since 1994 and remains the most connected building in Europe. It is also an integral part of Telehouse's expanding Docklands campus - the most connected data centre campus in Europe.

"Telehouse North has been a popular destination for carriers since the 1990s and this refurbishment is in direct response to customer requests to be part of that community," said Mark Pestridge, senior director, customer experience at Telehouse UK. "It gives more customers the opportunity to scale up and benefit from being interconnected in a carrier-neutral facility. It's also a major step in our continued expansion, which includes investing in new facilities like Telehouse South, alongside the modernisation of legacy buildings such as Telehouse North."

This is the latest development in Telehouse's European growth strategy, which includes the recent expansion of its Paris data centre and the forthcoming launch of Telehouse South in London. Telehouse South, the organisation's fifth data centre in London Docklands, is set to open in early 2022.

Telehouse is said to be the number one connectivity provider in Europe through its infrastructure positioning on the main backbone of the global internet (London-Paris-Frankfurt). Its continued expansion will see Telehouse double its capacity at all its existing sites in Europe over the next five years. ■

CityFibre donates access points to hospice

Independent full fibre platform CityFibre has supported staff and patients at a home providing care for the sick and terminally ill by donating wireless access points to boost coverage and overcome poor quality signal struggles.

Teesside Hospice, based in Middlesbrough, provides essential care for people and families who are living with a terminal illness. It has been suffering with poor signal quality, causing disruption to key processes, including logging medical records and internal communications, as well as limiting the online experience for patients. The donation will give all internet users access to better connectivity ahead of CityFibre's full fibre rollout in the area.

Teesside Hospice is in the planned build area for CityFibre's full fibre rollout, meaning the building will soon have the option of switching to full fibre enabled services. Construction of CityFibre's £42m network formally began in May and upon completion, it will be in reach of nearly every home and business in the town.

"We're proud to support the essential work of Teesside Hospice and even more excited to one day connect them to our full fibre network, supercharging the way staff work, the care they can offer and the ability for patients to communicate with family and friends," said Steph Carter-Smith, city manager at CityFibre. "Ultimately, we're hopeful that the network we're building in Middlesbrough, as well as other locations throughout the UK, will enable quality of life improvements for lots of hospitals, hospices and care homes, making a huge difference."

Anne Cooling, head of corporate development, Teesside Hospice, added: "We want to say a massive thank you to City Fibre and MAP Group for their donations of Unifi access points that will significantly improve the Wi-Fi signal at Teesside Hospice. The current signal quality is poor and causing disruption to patient and visitor communications and having an impact on the efficiency of nurses taking notes for medical records." ■

(L to R) Debbie Coulson, director of income generation, Steph Carter-Smith, city manager for CityFibre and Anne Cooling, head of corporate development

Mavenir to deliver UK's first off-shore Open RAN-based vRAN private network for windfarm connectivity

Cellular system integrator Vilicom has selected US specialist Mavenir to provide a private LTE network based on open RAN architecture for an off-shore wind farm in Scotland.

The project is the first of its kind in the UK, the companies said, combining open RAN in an off-shore private network.

Texas-based Mavenir said its virtualised (software-based) MAVair open RAN platform, working with commoditised radio hardware, will form the basis of a new LTE connectivity platform for sea vessels and workers within the boundaries of the Moray East offshore wind-farm project, off the coast of Scotland.

The Moray East wind farm is projected to deliver approximately 40% of the total electricity demand in Scotland, said Mavenir, powering the equivalent of up to 950,000 homes (out of 2.64 million dwellings in Scotland). This new private LTE network will also allow workers to connect on a regular basis through video calls and emails whilst they are at sea.

Designed with "cloud-native virtualisation techniques", the MAVair product enables the RAN to flex and adapt based on usage and coverage. Reading-based Vilicom sells indoor and outdoor cellular systems. It claims to serve "some of the biggest (and, indeed, the smallest) technology-driven companies in the world".

"Private networks are increasingly becoming more prevalent and we look forward to collaborating with Vilicom to develop further such use cases and applications," Stefano Cantarelli, chief marketing officer at Mavenir, said: "This project highlights the relevance and importance of advanced communications in a real application scenario." ■

Darlington Building Society hires 8x8 for digital transformation

Business communications and SaaS provider 8x8 said Darlington Building Society (DBS) selected 8x8 XCaaS (experience communications as a service) to support the organisation's digital transformation efforts.

Due to the sensitive and high-value nature of daily calls, the institution needed a robust communications and customer engagement system that could reliably handle steep call volumes, facilitate employee collaboration and provide secure payment options, regardless of where employees and customers were located.

DBS selected 8×8 XCaaS, which includes integrated contact centre, voice, video meetings, and chat capabilities. It implemented 8×8 across the entire business, ensuring that callers are quickly directed to the correct person. Staff can communicate and collaborate from anywhere and with 8×8 Secure Pay, the DBS' employees can provide "reliable and secure payment options to their members".

Sara Robinson, savings support operations manager at DBS, said the company chose 8×8 because of its single, integrated cloud platform and deep financial services industry expertise and experience.

"We deployed in July 2021 with head office and branch numbers staying the same, ensuring a smooth transition as members are still able to communicate with us easily," she said. ■

Allvotec & Vapour partner to accelerate next generation UC integration

Allvotec, an ICT specialist for major service providers, has partnered with disruptive cloud specialist Vapour, to bolster its unified communications portfolio.

As the market's retirement of legacy systems continues at pace, in favour of next generation, cloud-based UC adoption, Allvotec "sought to collaborate with a UC specialist to accelerate its innovation roadmap," it said.

Vapour has been appointed as a select partner for Avaya projects with less than 250 users. The Vapour Subscription Service (VSS) means Allvotec can securely deliver enterprise-grade UC services via Vapour's private network infrastructure, with an end-to-end service wrap, complete with SIP if required.

"For three decades, we've delivered, supported and maintained tech solutions that enhance customers' communications, collaboration and productivity, via a partner-exclusive business model," said Allvotec's CEO Dave Gardner. He added: We only collaborate with true experts who are as confident and experienced in their respective fields, as we are. We're forecasting a big growth over the next 12 months, as organisations' digital transformation projects continue at pace. Vapour will now play a key part in accelerating our ability to innovate, and deliver successful UC solutions which are agile, robust and compliant."

Vapour's CEO Tim Mercer added: "Today's UC offerings don't always meet the needs of partners and their end users. However, with businesses demanding better quality cloud voice solutions than ever before, this is a great opportunity for a 'Vapour x Allvotec' collaboration to drive change in the market. Together, we can deliver enterprise-grade Avaya tools to Allvotec's customers, while they retain complete control of the relationships they've built over the years."

Tim Mercer, CEO, Vapour

Originally specialising in secure cloud voice, video, networks and storage, Vapour revealed a new tech toolkit at the turn of 2021, which now includes SD-WAN solutions, a technology as a service offering, TeamsLink integration to supercharge customers' MS Teams capabilities and more. ■

EDITORIAL:
Editor: Robert Shepherd
roberts@kadiumpublishing.com
Designer: Ian Curtis
ian@firstsightgraphics.com
Contributors: Keith Ali, Sean Deuby, Nathan Wenzler, Mark Hardy, Mike Campfield, William Sword, Joost Grillaert, Christian Schillab and Nick Dobrovolskiy

ADVERTISING & PRODUCTION:
Sales: Kathy Moynihan
kathym@kadiumpublishing.com
Production: Suzanne Thomas
suzannet@kadiumpublishing.com
Publishing director:
Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Image Court, IC113, 328/334
Molesey Road, Hersham, Surrey, KT12 3LT
Tel: +44 (0) 1932 886 537

ISSN: 2052–7373

Birmingham University opens AI and data centre

University of Birmingham has opened an institute for the use of big data and artificial intelligence (AI) in a bid to address major global challenges.

The Institute for Interdisciplinary Data Science and Artificial Intelligence will put research on data and AI into practice through work with businesses and industry, charities and the public sector, it said.

Existing university partner the Alan Turing Institute, will work with the new institute on collaborative research in areas such as behavioural data science, healthcare, imaging and linguistics.

The institute will also work across the university and use data science to help with scientific research, medical diagnostics and robotics, as well as developing and training students in AI and data science.

Furthermore, the university's computing facilities, which are run by the Birmingham Environment for Academic Research, will also be used by the new institute, including the supercomputer BlueBEAR.

"Data science and AI have made spectacular advances in recent years to become vital tools in scientific research," said professor Iain Styles, director of the Institute for Interdisciplinary Data Science and Artificial Intelligence. "We're able to build on extensive expertise in modelling, statistics, machine learning, linguistics and optimisation – as well as the social, ethical and legal implications of data science technologies – to ensure these tools can deliver the information that we need to drive change."

Birmingham is a world top 100 university and part of the prestigious Russell Group. ■

Boots makes NICE move

Pharmacy and beauty chain Boots is among the first businesses to join an innovative program to streamline collaboration on investigations with UK police forces.

The NICE Investigate Digital Evidence Management solution from US technology firm NICE enables enterprises to work collaboratively on investigations to speed the delivery of justice, by ensuring fast, seamless sharing of CCTV video and other digital evidence. Boots has embraced the initiative by registering its thousands of CCTV cameras with the NICE investigate system. The initiative is being driven in part by the National Business Crime Centre, a UK resource created out of Home Office Police Transformation Funding.

Nasstar completes KCOM deal

Broadband and communications provider KCOM has completed the sale of its national ICT business to Nasstar, the companies confirmed.

The deal, which was announced in June 2021, has made the buyer one of the largest independent providers of managed services in the UK with more than 1,200 employees.

Nasstar will also become part of the NHS Health and Social Care Network (HSCN) with it fully accredited to provide and deploy HSCN network services to the health and care sector across the UK.

The existing KCOM National ICT services business will fall under the Nasstar brand within three months.

KCOM said the sale would allow it to focus on its core strategy as a regional provider of full fibre broadband to retail and wholesale customers.

"The sale of our national business reflects a refocusing of our business on our core priorities of expanding our regional network, developing our wholesale business and providing high quality, award-winning services to our retail customers across Hull, east Yorkshire and north Lincolnshire," said KCOM chief executive Dale Raneberg said. "Over the past 18 months we have made full fibre broadband available for the first time to homes and businesses in 20 towns and villages across East Yorkshire and North Lincolnshire as part of our £100m investment in our network expansion."

Wayne Churchill, chief executive at Nasstar, added: "We have been delighted with the feedback from customers since we announced the acquisition, and this has helped move the deal to completion quickly. We now look forward to the future and realising the value and opportunities the combination of KCOM's people, capabilities and customers represents." ■

FROM THE COVER

SDWAN REMOTE Relegates VPNs

SDWAN REMOTE - the simple, secure, cloud-managed connectivity solution that enables remote employees to work from anywhere using any type of connections with superior application performance and reliability. SDWAN REMOTE starts from £15 per user per month and is a fully managed solution that is available for 10 users or more.

Corporate VPNs were only ever meant to cater for 10 - 15% of staff working off site. But today's reality is that up to 100% of all staff may be required to work from home or remotely. This is where IT, finance and compliance teams start to uncover problems. Corporate VPNs are labour intensive to manage, expensive to upscale due to the requirement for VPN concentrators and VPN user issues can make a remote worker unproductive for days. Just like MPLS is not suitable to access Cloud applications and company VPNs were never designed for remote workers. Remote worker VPN support alone is stretching most IT departments to capacity. But these are not the only problems that VPN users face.

Backhauling traffic like Teams, Zoom, SFDC to the VPN concentrator and then on to the Cloud environment adds latency and bottlenecks, slow VPN speed frustrates workers and lowers productivity PLUS some workers have limited Internet access at home, frequent service interruptions and have to share Internet with the rest of their household.

SDWAN REMOTE from SDWAN Solutions eliminates all the problems above with a deviceless SD-WAN remote user solution. All the benefits of SD-WAN, all the functionality of a secure VPN with less problems, more efficiency and better performance.

SDWAN REMOTE is a software client that is downloaded onto users' mobile phone and windows PC simply by IT teams assigning user licenses using corporate email addresses. It's as easy as that. SDWAN REMOTE automatically provides encrypted access back to the corporate network and by combining intelligent session-based path steering with dynamic link conditioning and boosts the performance for latency sensitive applications.

Users can work from anywhere, using any connectivity available and bonding different connections to boost access. The SDWAN Solutions tech team have tested the solution rigorously with ethernet direct into a router, with home and guest wi-fi, and with 4G from a router and from even a mobile phone.

SDWAN Solutions are the trusted experts in all things SD-WAN and SASE, bringing tailored multi-vendor solutions from 10 top SD-WAN and 3 security vendors to market, along with a host of innovative solutions and products.

'Bad bots account for almost 40% of internet traffic'

Almost 40% of all traffic on the internet is "bad bot" activity, according to a report published by Barracuda Networks. Automated bots, including those from search engines and social media networks, make up 64% of all internet traffic. The Bot attacks: Top Threats and Trends report found that only a quarter of this was "good bot" activity - nearly two-fifths (39%) were from "bad bots." The report said these bad bots included basic web scrapers, attack scripts, and advanced persistent bots. "These advanced bots try their best to evade standard defences and attempt to perform their malicious activities under the radar. In our dataset, the most common of these persistent bots were ones that went after e-commerce applications and login portals," the report said.

'Half of IT leaders hesitant on future digital transformation programmes'

Nearly half (44%) of UK IT decision makers (ITDMs) are less confident in taking on digital transformation programmes due to negative past experiences, according to new research from Citrix. The new data was obtained through a study by Vitreous World, polling 500 IT decision makers at large organisations (250+ employees) in the UK, and aimed to reveal the extent to which previous experiences impact willingness to take on new digital transformation programmes. The poll revealed that even though many ITDMs have previously been involved with successful programmes, over half (51%) have been 'burned' by digital transformation projects that did not go according to the initial plan.

Fibre broadband network hits 50,000 premises

Extreme Networks has completed the acquisition of Ipanema, the cloud-native, enterprise SD-WAN division of Infovista. The acquisition expands Extreme's ExtremeCloudä portfolio, offering new cloud-managed SD-WAN and security software solutions required to power the Infinite Enterprise. Extreme will augment its ExtremeCloud portfolio with Ipanema's SD-WAN capabilities, "adding more flexibility, capability, and security when connecting locations, applications and devices", it said. Extreme said the acquisition accelerates the company's goal of bringing distributed connectivity, security, and cloud capabilities to customers. The acquisition establishes a second technology centre of excellence for Extreme in Europe and deepens the company's customer presence in that region. Ipanema has more than 400 customers and its solutions are deployed across more than 100,000 sites. Extreme plans to leverage Ipanema's existing relationships with leading MSPs and XSPs as part of its go-to-market strategy across EMEA.

Stellium opens new Aberdeen office

Stellium Data Centres has opened a new Scottish office in Aberdeen, as part of its growth strategy for the north of the UK.

The group, one of the largest purpose-built co-location and network providers on these shores, said the Scottish market is important for expansion plans, as it aligns with the evolving macro data centre market, both regionally and internationally.

Developments in submarine networking with the Denmark-UK North Sea Connect and Norway-UK subsea cable systems at Stellium has led to Scotland becoming one of the best connected data centre hubs on the continent.

"This an exciting time for Stellium as the company continues to experience rapid growth," said Gerry Murray, chief operating officer at Stellium. He added that Stellium is committed to being part of the growth of the Scottish ICT sector, "the enhancement of the Scottish data centre proposition and national and international connectivity in the region".

New device to counter USB drive cyberattacks

A team of scientists at a UK university has created a sophisticated new device to counter the cyber threat posed by malicious USB drives. This 'external scanning device', designed by experts from Liverpool Hope University, has been granted a patent from the government of India and will soon move to production. The project is being led by Shishir Kumar Shandilya, a visiting research fellow in Hope's school of mathematics, computer science and engineering, alongside professor Atulya Nagar, pro-vice-chancellor for research and professor of mathematics at Hope.

Fibre broadband network hits 50,000 premises

Netomnia the Cheltenham-based fibre network operator. has just passed 50,000 businesses and homes across its rollout areas, having added 20,000 premises to its network in the last two months. The firm is now delivering its infrastructure in 14 towns across England, with more to come over the coming months, as it aims to connect 100,000 premises by the end of 2021 and one million by 2024. Founded in 2019, the company is making multi-million pound investments across the UK and is aiming to prioritise cities and towns, previously left behind by other operators, where the existing mixed-copper-and-fibre or cable infrastructure cannot provide the future-proofed connectivity demanded by an ever-more digital-reliant economy.

UK to overhaul privacy rules

The UK will attempt to move away from European data protection regulations as it overhauls its privacy rules after Brexit, the government has announced. The freedom to chart its own course could lead to an end to irritating cookie popups and consent requests online, said the culture secretary, Oliver Dowden, as he called for rules based on "common sense, not box-ticking". However, any changes will be constrained by the need to offer a new regime that the EU deems adequate, otherwise data transfers between the UK and EU could be frozen. John Edwards, currently the privacy commissioner of New Zealand, will be put in charge of overseeing the transformation. He will replace Elizabeth Denham, whose term in office will end October 31 after a three-month extension.

Word on the web...

Playing catch-up to early adopters

By Sarthak Rohal, VP - IT services at AlphaCodes

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

WatchGuard Endpoint Security Solutions

Confidently protect your devices

WatchGuard Endpoint Security Cloud-native solutions protect businesses of any kind from present and future cyber attacks by delivering the Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) solution. Our WatchGuard Endpoint Security platform offers comprehensive EPP and EDR protection as well as threat hunting and zero-trust application services, delivered via a single lightweight agent and managed from a single pane of glass.

WATCHGUARD EPP

Endpoint Protection Platform

WatchGuard EPP is an effective Cloud-native security solution that centralizes next-generation antivirus for all your Windows, macOS and Linux desktops, laptops, and servers.

WATCHGUARD EDR

Endpoint Detection and Response

WatchGuard EDR complements other EPP solutions by adding a full stack of EDR capabilities to automate the detection, containment, and response to any advanced threat.

WATCHGUARD EPDR

Endpoint Protection Detection and Response

WatchGuard EPDR combines our broad set of EPP technologies with our EDR capabilities for computers, laptops and servers to detect threats that traditional solutions cannot even see.

Threat Hunting Service

Zero-Trust Application Service

+44 (0) 203 608 9070

uksales@watchguard.com

Improving your security posture with hybrid identity protection

By Sean Deuby, director of services at Semperis

Covid-19 has often been cited as the catalyst accelerating pre-existing trends in the past 18 months, with ecommerce and automation two of many multiple markets championing this school of thought.

The widespread shift to remote and hybrid working models, however, was less acceleration and more holistic transformation born out of necessity. Prior to the pandemic, only 4% of Europeans worked from home, but when the pandemic struck this figure rose to 88% of staff.

As organisations were forced to adapt almost overnight, IT professionals were called into action, taking a variety of different approaches to ensure the continuance of operations on a remote basis. Those in more heavily regulated markets such as financial services enhanced their virtual private networks (VPNs) as a means of maintaining access to SaaS applications through the corporate network. Meanwhile, more agile markets and enterprises that were previously considering shifting to cloud-first IT policies were compelled to adopt them when staring down the barrel of a national lockdown.

In both instances, cloud-based single sign on (SSO) capability – providing users with remote access to their corporate networks with the same credentials they use on premises – is vitally important to security.

To achieve SSO, a hybrid identity architecture that projects an organisation's credentials into the cloud service is required. Yet hybrid identity presents its own challenges.

Not only is it more complex, most hybrid identity architectures depend upon Microsoft Active Directory (AD) – the most widely used on-prem identity system in the world, and a foundational piece of IT infrastructure for roughly 90% of companies globally.

The problem with Microsoft AD is that it was rolled out over two decades ago, in an era where the IT landscape looked entirely different. Simply put, Microsoft AD is not prepared for today's intense threat environment.

Hybrid identity was a key vector in the SolarWinds breach

AD was designed to make resources easily discoverable to domain users, and therefore still supports several legacy applications that require insecure authentication protocols such as NTLM. Over time these legacy-based security gaps can accumulate, creating a series of configuration weaknesses and multiple hard-to-protect points of potential entry for a cyber attacker.

A prime example of an AD-related breach is the SolarWinds attack, one of the most malicious supply chain attacks seen to date, which first came to light in late 2020.

After successfully infiltrating SolarWinds' systems, the threat actors implemented malicious code into its Orion software – a network management tool used by 33,000 of the company's customers.

When the next regular Orion software update was released, the tampered code created a back door that allowed the hackers to access the IT systems of 425 Fortune 500 companies and US government agencies, where they were able to deploy even more malware.

Crucially, AD was used to conduct internal reconnaissance, elevate privileges, and gain administrator access to the organisation's domain. In turn, the SAML signing key of the organisation's AD FS servers was stolen, enabling the execution of a Golden Ticket attack against its Microsoft 365 environment to gain access to corporate email.

Response is as important as prevention

Albeit an extreme example, the SolarWinds attack is just one of countless AD-related incidents that happen every year.

According to Mandiant researchers, approximately 90% of all businesses are exposed to security breaches as a result of AD mismanagement, while 9 in 10 of all attacks involve AD in some capacity – either as the initial attack vector, or a means of manipulating and elevating privileges.

But AD is not going away. If on-premises operations exist, AD will prevail.

So, what is the solution?

At Semperis, we've created Purple Knight – a free, easy-to-use assessment tool that companies of all sizes can leverage to perform AD-centric security analysis. Yet this assessment is just the first step.

Organisations need an end-to-end strategy for defending against cybercriminals before, during, and after an attack. In addition to tools for identifying security gaps, security and identity teams need solutions for detecting attackers that have breached the network and are moving laterally through the system. Catching threat actors before they unleash malware can be tricky: Many malicious AD changes fly under the radar of traditional SIEMs.

Once the system is breached, organisations understandably focus on resuming business operations as quickly as possible. But that approach can backfire: Threat actors will often reside in a network for weeks or months, understanding exactly what value they might be able to extract before detonating a malware payload. Without appropriate response planning, AD domain controllers restored from traditional server backups will more than likely contain the same malware – thus starting the attack cycle all over again.

Shift to remote work raises the stakes for defending against cyberattacks

As the shift toward at-home working continues, and the network perimeter dissipates, identity has become a primary line of defence against cyberattacks.

It is therefore vitally important that companies understand this shift. ■

From survive to thrive: unlocking ROI from remote working

Keith Ali, MD at Creative ITC

Following the pandemic-driven rush to ensure business continuity, many IT teams have ended up managing an unplanned mix of technologies. Now, with organisations transitioning to long-term remote and hybrid working models, they're facing a new challenge - choosing a sustainable solution that improves workforce mobility and productivity without increasing cost and complexity.

Organisations are increasingly choosing virtual desktop infrastructure (VDI) as a long-term, scalable solution where upfront CapEx costs are largely replaced by OpEx. But, the pandemic's shakeout means financial approval for any IT investment is often tougher than before - especially if you're pitching to a C-suite still reeling from balance sheet challenges. So, what's the best way to build a business case for the remote working long haul?

You can't ignore the fact that VDI adoption in some industry sectors has been problematic. IT teams discovered off-the-shelf VDI platforms were unable to cope with the demands of power users dealing with graphics heavy applications. Many Architecture, Engineering and Construction (AEC) firms, for example, failed to deploy VDI successfully for users of CAD applications handling huge BIM files, giving remote workers a hindered experience and preventing collaboration. The result is that these power users have become effectively shackled to their office IT.

To overcome board level and user reluctance arising from bad experiences, it's now crucial for IT teams to choose an effective VDI solution for all users to unlock return on investment.

In the right hands, VDI can be engineered for the most demanding of settings. Purpose-built solutions now provide super users of big data or graphics-heavy applications with tools and experiences identical to or better than they enjoy in the workplace.

Look for a supplier with a successful track record in your sector, one who fully understands virtualisation in the cloud and how industry-specific applications and network services behave together. Their experience will be invaluable in unlocking the full potential of VDI.

Deployment models should be tailored to individual business needs, where IT teams are free to decide which workloads to deploy in the cloud and which to retain on-premise. To optimise ROI, look for a provider offering consumption in the cloud, on-premise, or using a hybrid model in a single seamless solution.

Decide who manages what: in-house managed options such as Windows Virtual Desktop (WVD) or on-premise VDI, or Desktop-as-a-Service supported by a VDI specialist? Be honest about your in-house skillset. The MSP route can dramatically improve the business case with savings on data centre space, infrastructure, upgrades, licensing, application deployment, support and headcount.

Most organisations realise a better approach for overcoming approval hurdles and getting the best results from VDI investment is to build support based on a specialist provider's ability to unlock much greater value for around the same outlay.

A business case for any IT investment must, of course, be founded on a solid financial argument. Beware of providers offering VDI solutions designed solely with money saving in mind. Before and after IT infrastructure costs can remain flat or even rise slightly.

Be careful not to compare apples with oranges. In moving from on-premise VDI or WVD managed in-house to Desktop-as-a-Service delivered by an MSP, start by calculating the total cost of ownership (TCO), usually over a five-year period. In-house expenses should include PC hardware refreshes, virtualisation software and additional GPU, together with costs associated with system administrator salaries, power, rack space, out-of-hours staffing and training costs to support the deployment.

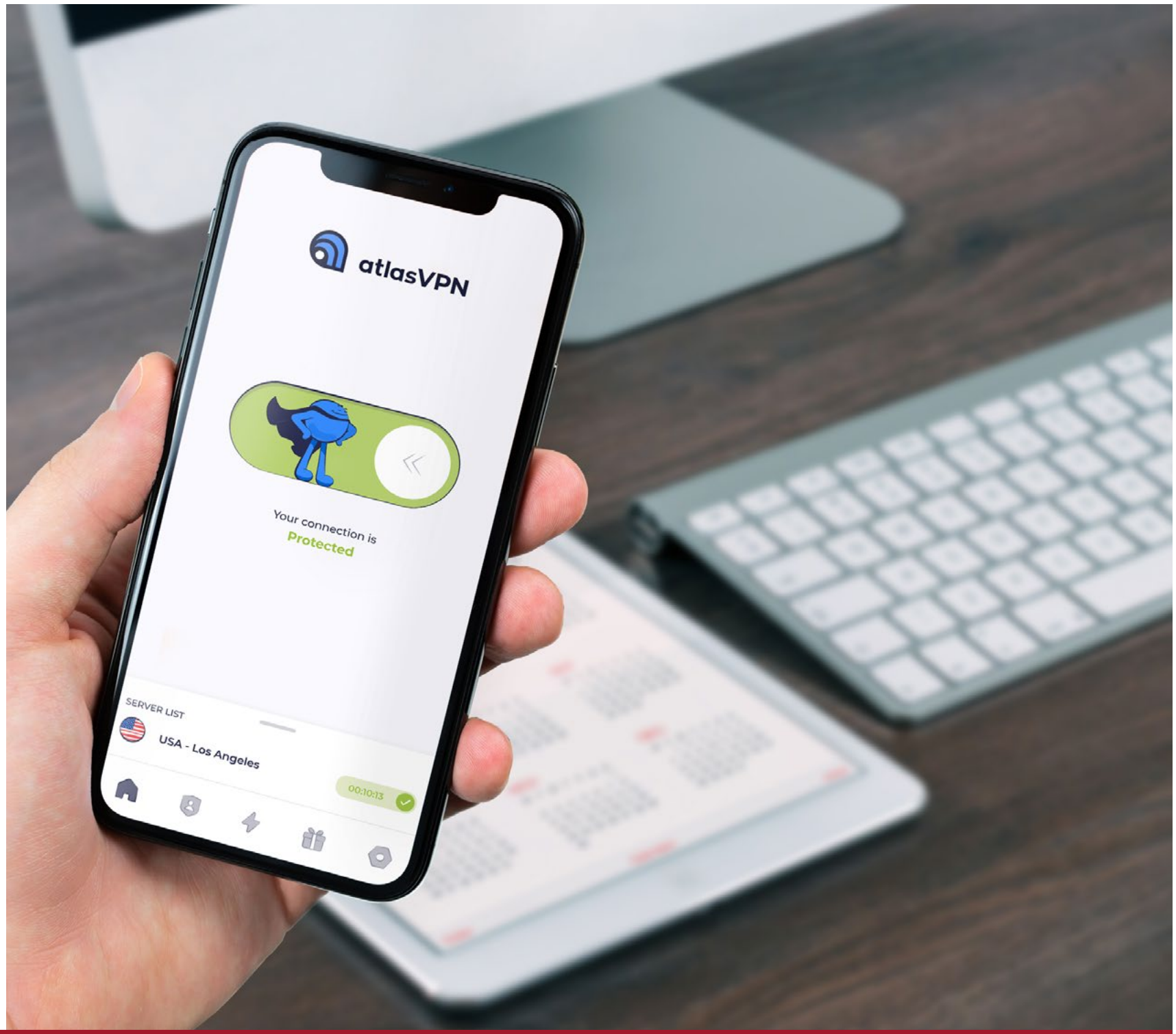
Not all external VDI providers offer the same value for money. Scrutinise their technical credentials and be confident they can deploy the right solution and provide ongoing management, optimisation and support. Make sure you'll benefit from the latest technologies and regular updates during your contract.

Many providers differentiate between VDI profiles for ordinary and power users. To reduce TCO further some VDI specialists have taken cost-effective consumption to another level by offering scalable pricing. Clients pay per user, per month, per profile by purchasing credits that IT teams can stipulate and reallocate any way they like. Creating VDI burst capability and instant scalability for fast-changing business needs.

Factor in technological gains like enhanced data security, built-in disaster recovery, faster IT provisioning, speed of access, improved version control and time saved eliminating rework and duplicated effort.

End-user productivity gains are often overlooked. The value of enabling project teams to work and collaborate effectively from anywhere should not be underestimated. For example, designers and engineers in different time zones can work together on complex 3-D building models, delivering critical construction projects faster at less risk and cost. Similarly, in healthcare settings, MRI scans can be shared by radiologists and department specialists – on devices anywhere – improving clinical decision-making and expediting treatments.

A business case based purely on financial costs ignores a host of wider benefits. Taking a holistic approach to VDI investment will result in a compelling case demonstrating clear ROI, enabling your organisation to not only enable remote working, but actually to leverage it. ■



VPNs: security, speed and how to choose a provider

VPNs are very popular with consumers wanting to unlock a world of streaming content, but why do enterprises need them? Robert Shepherd investigates

If you stopped the average person in the street and asked them what a VPN (virtual private network) is, you'd either get a short, shrift "no idea" or a "yes", followed by a comment on how amazing they are. I know, because I've asked. I also know because I have one.

However, the people in the latter group (except me) are most likely to use one for their viewing pleasure. That's because nowadays VPNs are synonymous with unblocking geo-restricted content by succesfuly navigating local licensing laws. You could say it's often used to stream content illegally (definitely not by me).

However, we're not here to talk about how some people access their favourite TV shows, nor to learn about their viewing habits, but to ask how businesses use VPNs.

Think back to that dreadful first quarter of 2020 and the arrival of the novel coronavirus. For the first time ever, almost every single industry was forced to re-think operations. How would we all work if we couldn't make it to the workplace?

We all headed to our respective remote offices (bedrooms, living rooms and kitchens in many cases) and it was VPNs that made it possible for us to work as usual. Granted, not every enterprise had a VPN in place, but those that did provided their staff members with a secure way to connect to the company network to access systems, data and files.

Now, some 20 months later, remote working is a permanent solution for many businesses - and that means a secure remote workforce.

It's also important to remember that VPNs are nothing new. To the consumer,

maybe they are, but VPNs were actually designed and introduced almost 20-years-ago for connecting devices with on-premises networks. To this day they are a highly mature technology – but with today's cloud-based infrastructure (public, private and hybrid), they are attempting to protect an environment they weren't really built for, which, according to some, can be a boon for attackers. Instead of protecting a flat network with linear access, some VPNs are now used to protect the perimeter network.

So, what does that actually mean? Are VPNs still an integral part of a business with lots of staff working remotely, or have they had their time?

William Sword, cybersecurity writer and researcher at Atlas VPN, argues that enterprises should use a VPN as it encrypts data on all of the devices in the company's network. "That way, hackers or internet service providers would not be able to see your data," he says. "Employees would always access the internet through a secure and private connection."

Nathan Wenzler, chief security strategist at Tenable agrees and presents a slightly more technical explanation.

"VPNs create a connection between two endpoints that is, as the name describes, private," he says. "Whether this connection is across public networks - like the internet, or internally to a corporate network, VPNs facilitate an encrypted tunnel that secures the communication in transit between the two systems. This is an incredibly important security tool which enables remote workforces to connect to corporate data and assets from outside the corporate network without exposing the data or other information to anyone else in the public space."

It goes without saying; any tool that encrypts company data is always welcome. However, VPNs are not without their detractors – often because they slow down the whole internet experience. Just ask anyone trying to stream a TV show or movie.

There can be a number of reasons behind it, such as the wrong choice of server location. The further the server is from your true location, the slower the speed. The data packet must travel a greater distance and the speed of the VPN connection may slow down significantly and ping may reach critical levels.

Of course, speed and latency are not helped by the fact that so many workers are increasingly taking advantage of the flexibility of working from home. Throw Zoom meetings into the equation and you potentially have a perfect storm. After all, fibre-to-the-home can have bandwidth issues at the best of times.

It's hardly good for businesses, is it?

"End-user trust is strictly based on the notion of access to the corporate network"

Mark Hardy, Citrix

"When using a VPN, it is absolutely normal for the internet to be a bit slower, but it should never make your browsing frustrating," adds Sword. "In fact, I can assure you that having a bit of a slower internet is much better than losing your or even your customer's sensitive information due to security vulnerability."

Wenzler concurs and says for most countries across the world, speed and latency isn't really an issue for VPN use any longer – and here's why. "In the early days of broadband, where download and upload speeds were very limited, the overhead generated by VPNs could impact performance noticeably," he continues. "But, as the vast majority of offices and homes have fast Internet connectivity (at least in relation to the early days) coupled with the overall improvements VPN providers have made over the years, speed and latency shouldn't be an issue for most every use case."

Now that you know – if you didn't already – why your business could do with a VPN, you're likely to ask how you start looking for the right provider.

Just a few years ago, a quick internet search would reveal a handful of VPN companies. Google the term now and you'll find yards of text, news and reviews telling you which companies are good, which ones to avoid and the ones offering the best value for money when it comes to enterprises.

So, how do you choose between them?

Sword is a good person to ask because he works for a provider.

"When choosing a VPN, enterprises should choose a service that comes with a no-logs policy," he says. "In addition, I would highly recommend a VPN that has a centralised management panel. IT admins can add or remove accounts from the console and check what devices are connected to the VPN. Lastly, I would mention to check the features the VPN service is offering, Killswitch, different protocol options, wide server variety are all good signs of a quality VPN. "Some VPNs offer features like a data breach monitor, which scans the web and checks whether your personal information is leaked online. With such a feature, employees can make sure their data is safe."

Another security framework associated with remote working is what's known as zero trust.

It operates by assuming that the device or user is not authorised for access, and then authenticating each connectivity request. This approach limits the surface area and provides the necessary scalability. Zero trust also provides visibility into every user and device that VPNs lack, which allows a greater level of protection — more so for personal devices. In addition, security experts collect behaviour analytics to combine with artificial intelligence that can help proactively prevent future attacks. With working together being an increasing part of businesses, zero trust also allows companies to securely provide as-needed access to partners, vendors, customers and contractors.

Due to the boom in remote working, many companies have shifted and continue to shift to zero trust.

So, how does it compare to a VPN?

"When comparing VPN with zero trust security, I would say both of them are equally important," says Sword. "VPN provides employees with secure remote access to company resources, while zero trust security fills the gaps in traditional network security architectures to prevent any inside or outside attacks."

For Wenzler, it's not even a debate because in his view, "comparing VPN technology to zero trust guidelines and principles is very much an apples-to-oranges comparison". He says "zero trust is more of a mindset or overall philosophy" that provides a guide toward how an organisation approaches its entire security program "while VPNs are technologies that provide a very specific form of security control. Looking at it from a People-Process-Tools spectrum, zero trust is a process while VPNs are tools. That said, VPNs can be a part of an organization's zero trust initiative and would support some of the guidelines around securing communication or providing access on a per-session basis, but they should not be the sole security control used to address the various processes and requirements needed to properly implement a zero trust security program across an enterprise."

While the zero trust and VPNs are quite different, one of the many ongoing security debates is how best to use them together.

On the face of it, it's seen as most helpful in the short term while moving to a zero trust approach, which can be lengthy due to how complex the shift can be. While a VPN simply provides access to remote users and zero trust is a holistic authentication approach, VPN can be used as an access method as part of zero trust. However, once the zero trust framework is rolled out, it's much less time consuming to scale and grow the framework.

However, Mark Hardy, director of cloud networking at Citrix, argues that IT security solutions are not made for hybrid work.

He says that's because traditional VPNs are designed for the occasional remote worker, not for many or even all employees working from home. "This is why more and more businesses are looking for a security solution that actually fits the age of remote working," he adds. "Zero-trust brings security controls from the network or VPN level to the application level, and from an initial all-access security check to granular rules and permanent monitoring. For a zero-trust security infrastructure, it doesn't matter where, with what devices, or via what kind of network connection employees are accessing their business applications and internal data – all access is treated in a 'never trust, always verify' manner to ensure the highest standard of security while working remotely."

Hardy explains how the VPN model has worked for use cases where end users get access to the corporate network, typically from approved corporate-managed devices only. "End-user trust is strictly based on the notion of access to the corporate network," he continues. "Classic VPNs do not align with zero trust principles, since one-time access gives a user the metaphorical keys to the kingdom. Instead of this castle-and-moat approach, the zero trust model will use a dedicated VPN-less proxy that sits between user devices and the full spectrum of applications they need, from enterprise SaaS to unsanctioned web apps. This proxy can enforce granular cybersecurity measures, such as disabling printing, copying and pasting on an endpoint if the contextual evidence supports doing so."

"VPNs create a connection between two endpoints that is, as the name describes, private"

Nathan Wenzler, Tenable

Nevertheless, businesses need to look at the bigger picture: is the VPN secure and robust enough to protect against today's increasingly sophisticated threats? Last year, cyber criminals launched vishing scams specifically designed to gain sensitive information through the VPN. With so many devices and locations involved, VPNs create a very large surface to protect. If an attack occurs, the potential damage is significant — because VPNs often give users access to the entire network.

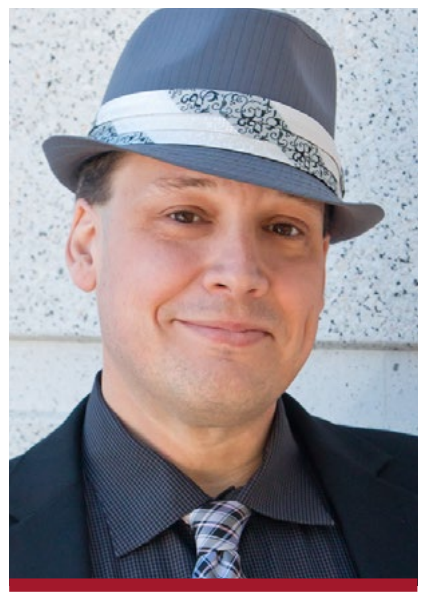
Mike Campfield, head of EMEA operations for ExtraHop, says it's important that companies should consider the pros and cons of VPNs. "When used properly, VPNs can strengthen an organisation's security and can be highly scalable," he adds. "A couple of advantages are that it secures the network by stopping hackers or software from accessing the organisation's connection and hides private information through encryption. But this encryption process takes time and can sometimes significantly slow down internet speed. Also, VPNs can't provide tailored access at the protocol or host level, potentially opening up users to services they shouldn't be accessing, creating new risks for the organisation."

Although VPNs have been viewed as the answer to supporting employees working outside of the office, Campfield says the biggest issues came about because of Covid. "They became overwhelmed throughout this shift, providing inbound security headaches alongside outbound challenges related to patching distributed endpoints," he concludes.

Think of a VPN as a curtain, stopping opportunists and professional cybercriminals from viewing your browsing activity. A good VPN will also secure your internet connection, protect your privacy and conceal your identity, keeping you safe from hackers or anyone else who might be trying to keep tabs on your online activity. In reality, it does more than just protect the network.

Nevertheless, it's important to remember that not all VPNs are created equal and each one comes with its own set of pros and cons.

Choose wisely. ■

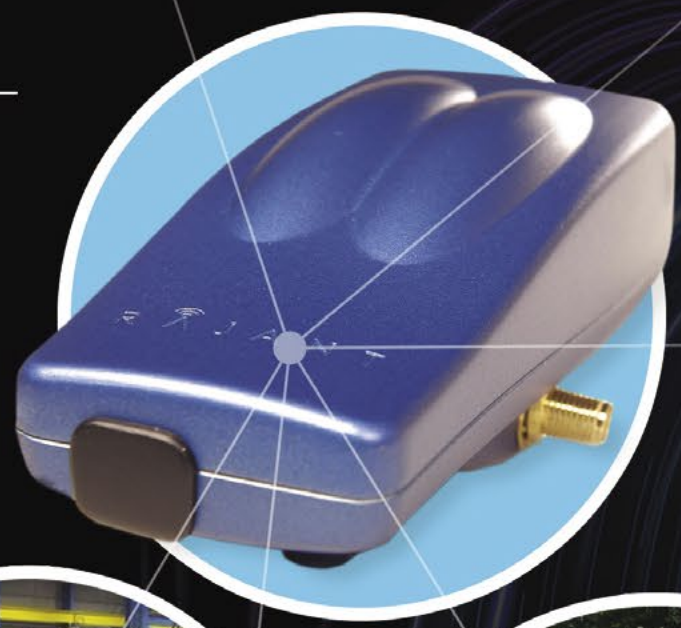


Just like today's industrial leaders, Rajant's network is

Smart. Autonomous. Always moving.

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

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



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

*Industrial Wireless Networks **Unleashed.***

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

RAJANT

School of thought

Three different institutions embrace the future of learning with much-needed upgrades

Implementation of wireless Infrastructure

The University of Huddersfield has an undergraduate and post graduate student population approaching 20,000. The institution achieved university status in 1992, but has its origins in a series of institutions dating back to the 19th century. Today the university is situated on the Queensgate campus, south-east of Huddersfield town centre. Almost all of the university's teaching takes place on the campus, split in two by the Huddersfield Narrow Canal.

The university has made substantial investment in a refurbishment and building programme over recent years, modernising and developing the estate and now has fantastic facilities including specialist laboratories, studios and performance spaces. university buildings range from an historic 19th century church through to modern buildings including the home of Art, Design and Architecture, the Barbara Hepworth building. The university has a long history from its founding as the Young Men's Mental Improvement Society in 1841 through to the present day.

The university has excellent standards of education, reinforced by numerous awards that it has received. These include the first Global Teaching Excellence Award, recognising the university's commitment to world-class teaching and its success in developing students as independent learners and critical thinkers in 2017. In addition, the university is the UK's leading university for the receipt of National Teaching Fellowships to mark Britain's best lecturers in Higher Education for the past ten years and is proud to have been recognised as a gold-rated university by the Teaching Excellence Framework (TEF)

The university had been experiencing issues with its ageing wireless LAN system, which although when initially installed performed well was now starting to struggle with the demands of a more mobile learning environment.

The university engaged with a number of prominent WLAN vendors, seeking to appoint a leading solution, fit to support the university in its delivery of first class teaching and learning. As part of this requirement the University asked vendors to engage with leading, trusted, reseller partners to develop and deploy a proof of concept, to provide a live test environment from which the University could evaluate the new solution in many forms.

Evaluation of the new solution would include ad-hoc reviews of service provision from both staff and students of the test environment, as well as more measured technical and performance reviews to demonstrate capability and functionality. Following review, the university signed a contract in the summer of 2018 with European Electronique to deploy an Aruba WLAN solution.

The solution selected by the university is from a portfolio of products by HPE Aruba rated by industry analysts Gartner and Forrester as market leading. The solution was architected and deployed by European Electronique for both the initial proof of concept and migration and deployment to the live environment.

The solution consists of a number of Aruba Mobility Controllers, deployed in a cluster running the latest AOS 8 software, supported by a Mobility Master to deliver a centralised dashboard to easily see and manage controllers and to provide live firmware and feature upgrades to improve network reliability during active user sessions.

In order to ensure that the new WLAN deployment was fit for purpose European Electronique surveyed the estate of buildings to determine optimal placement of access points. This survey covered the estate of approximately 1100 APs and was conducted across the University's range of very diverse buildings including old converted 19th century mill buildings through to modern, open plan, buildings. The surveys were documented and provided to the University for their existing cabling contractors to install both any new datapoints required to support the APs as well as the APs themselves.

Post installation surveys were initially commissioned by the university but were not all completed due to the University's satisfaction with the accuracy of the initial pre-installation surveys. European Electronique continues to support the university with post installation consultancy and support, as well as development of the solution to enable the university to build upon the initial deployment to provide further benefits and services to the university. ■

'Inclusion for all'

King James I Academy is a medium size academy and Sixth Form centre for students aged 11–18 in the town of Bishop Auckland, County Durham, with over 800 students in Years 7 to 11, and a further 160 Sixth Form students on roll.

Around five years ago, the school received funding through the Priority Schools Building Programme to replace one of its buildings with a new modern purpose-built set of classrooms as well as a refurbishment of its existing Grade II Listed building. This proved the catalyst to invest in a more modern technological infrastructure, with a reliable Wi-Fi network made up of 57 access points, and the then headteacher Mr Nick Grieveson (recently retired) made the decision to offer each new Year 7 student a Chromebook device.

About two years later – with the previous Year 7s now in Year 8 using their Chromebooks, and a new cohort of Year 7s issued with their own devices – the school also invested in RM Unify as the single sign-on access portal for all of their online software applications, and that made a huge difference to the user experience for staff and pupils.

The next decision was Google or Microsoft. Until this point King James was a Microsoft school, but with Chromebooks installed, it opened a new avenue of thought.

It was also time to look at the server infrastructure, with RM helping the school replace their servers with a RM designed Dell VRTX system with SAN and Backup – moving to CC-on-prem for remote access. By this point, the school had been investing in Chromebooks for several years as devices that pupils could use – initially for homework or as an extra resource in class. This 'Chromebook Scheme' was an initiative set up for each Year 7 cohort, with the aim that they would keep their devices throughout their time at King James. When the pandemic first struck and resulted in the first national school closure in March 2020 (to all but the vulnerable and children of key workers), King James mainly relied on its website and other platforms to set work for pupils to do at home. This was the best option at the time as not all students had access to a Chromebook or a device of their own.

It was at this stage that the school made the decision to audit student access to Chromebook devices for a more consistent learning strategy for remote learning. Parents had been asked to make a financial contribution in the form of a refundable deposit – in part to minimise the cost to the school, but also to ensure a joint commitment to such an expensive investment. This proved acceptable to most, with 95 percent of parents willingly paying the small deposit requested.

This was a significant project – to roll out devices right across the school – with a huge team effort supported by admin staff, IT technicians and a dedicated Chromebook liaison staff member (Laura Newton) who worked tirelessly to fill the gaps. By the end of September 2020, every student had a Chromebook. Whilst they continued to rely on parental contributions, the school also benefited from the DfE Laptops for Schools programme to provide devices for all, as well as Wi-Fi dongles for those with inadequate internet connection at home.

Under guidance from the leadership team, an internal champion was sought – a well-respected class teacher with a genuine vision for how this could work.

She researched the various platforms, as well as the pros and cons of each one. She looked at specific applications and identified opportunities such as Google Apps (now called Google Workspace) for Formative Assessment, Google Drive for students storing their work electronically as a long-term revision tool, and Google Classroom so all students could access remote learning resources and live lessons through Google Meet… concluding that this was the future of education and a space where King James could lead the way.

It became almost a production line – as the Chromebooks arrived from the various sources, the in-school IT team configured them to work with the necessary school software, cyber security and safeguarding programmes, before the project team allocated them to the next pupil in turn, ensuring they had been

trained in how to use them through whole school tutorials, and had the necessary logins and passwords.

By the time the third lockdown came in January 2021, the school was probably in the best position it could be – it had a cloud-enabled network, staff and students had access to devices, they had a remote learning platform, and everyone knew how to use it. The school had also purchased the new RM Tutor software application for Chromebooks, which syncs with Google Classroom in readiness for students returning to school. This proved very helpful for teaching and learning, as well as monitoring students while they were working.

One of the consequences of so many pupils now online is ensuring that safeguarding and policies are up to date. For King James this was made easier through Google Workspace, as the functionality that goes with that enables the local IT team to be able to control what a pupil can and cannot do within Google Classroom.

For King James they also make use of the RM Tutor Programme which allows a teacher at the front of the class to see exactly what each student is looking at, so that it can spot if a student is going off subject (such as playing a game).

That said, there were still many parents with concerns and worries about how their child might be using the devices. Fortunately, Google Admin Console provides a complete history of what sites a child has visited and what they have done on that site, as well as blocking those that are considered inappropriate. Google Admin Console is a useful application, as it allows a school much more control over student Chromebooks - once each Chromebook is enrolled, it allows the school to lock the device if it is lost or stolen, displaying a customised message on the screen such as "Please Return to King James I Academy" and advising that the Chromebook will be useless to anyone else. For King James, it had made the decision to work with a national technology partner many years ago, and over the years, RM has supported it in many aspects of its technology journey, with that support coming to the fore during the pandemic – sharing advice and best practice from other schools facing similar challenges.

One of the most important bridges for the school was RM Unify – having a single log-on that opened the door to all of the software applications that a student would need – from their email to their homework, and from specialised music applications to

being able to interact in a foreign language – it really did make it so much easier to get everyone on line in those early days.

For staff, it was CC4-on-Premise that proved the key application. Whilst they had it pre-pandemic, it was rarely used, but as soon as staff realised they could access all of their files and applications from home, it became a lifesaver for everyone. With CC4 it meant that the IT team could change people's passwords remotely from home – again allowing them to keep the school running seamlessly despite the constraints imposed by Lockdown.

Based on the buzz that is evident at King James it is clear that it will not be going backwards. For the academy, learning is now "blended" – whilst they are excited by what technology can do, they recognise that it cannot all be done on Chromebooks – pupils still need to be able to write with a pen. ■

Sustainability and a data solution for Oxford University's GLAM division

Oxford University's Gardens, Libraries and Museums division (GLAM) forms one of the greatest concentrations of university collections in the world. GLAM holds over 21 million objects, specimens and printed items, constituting one of the largest and most significant collections in the world.

Faced with the challenges of increased data demand, the Museum of Natural History – one of the museums within GLAM – wanted to upgrade its IT infrastructure to house core network switches, responsible for running the services. A major rewiring project was undertaken with the aim of significantly improving the data connectivity for computers, phones and next generation devices.

The wiring presented a challenge in itself as the historically significant listed building was not best designed to accommodate the space for conventional hardware. This required ingenious methods to work with the fabric of the building.

Faced with these challenges, Anjanesh Babu the technical project lead in the GLAM IT team, researched options available. The traditional approach was for the designated network core of a building to be stripped bare and rebuilt with air conditioning and electrics to meet the requirements for the equipment. However, given the nature of the building, this would present a number of challenges, including space and cooling loss through the surfaces.

Anjanesh Babu, technical lead for the project, approached Rittal's IT team who quickly identified the "Data Centre in a Box" (DCiB) concept as a possible option. DCiB replicates the key data centre capabilities but on a smaller scale and has been developed to enable equipment to be deployed in non-traditional Data Centre environments. The turnkey package concept provides IT Racks, demand-orientated climate control, PDU, monitoring and fire suppression. It provides a complete solution from product selection, through to installation and ongoing maintenance. When installed in the Museum of Natural History, the cooling footprint would be significantly lower than the traditional full-room air conditioning and the absence of any work to the space to accommodate the system would mean that the building would remain relatively untouched.

A site visit by Joel Farrington, Rittal's area sales manager for IT was arranged, and the requirements gathered. "The system was to be located in the museum's basement which had restricted access with very narrow staircase & doorways. In addition to this, the building's listed status would mean that any cooling equipment would have to be positioned cleverly and with the utmost

consideration, not only to aesthetic but to any noise pollution emitted" recalls Farrington.

Joel and members of the Rittal IT development team, Clive Partridge and Andrew Wreford, worked with Anjanesh Babu to identify key areas that needed to be achieved. "Given the kW loads & environment of the proposed location, it became clear that the DCiB's LCU option was the best way to go, and we quickly built up a package including racks, accessories, cooling, fire suppression, PDUs & monitoring. To mitigate the access restrictions, we used the 'rack splitting / re-joining' service which enabled us to resolve the challenge of space limitations of the project" says Rittal's technical IT manager, Clive Partridge.

Rittal provided an end-to-end solution from the manufacture of kit, to the installation, commissioning & hand-over. To overcome the issues with the listed building status, Rittal's IT team worked in collaboration with Babu and the lead contractor, Monard Electrical, to find a suitable home for the condenser.

Technical project lead from GLAM, Anjanesh Babu, reflected on the options deployed: "RIttal's DCiB allowed the museum to utilise the proposed location without having to make costly building modifications, thus saving time, energy and effort."

By adopting "in-rack" precision cooling instead of "in-room" cooling, the location is more environmentally efficient and this controls operational expenditure. Cooling via the high-performance LCU option provides temperature consistency, allows better care of their equipment along with nearly silent operations.

Not only is the installation providing energy efficiency and longevity for the museum, there is the added benefit of noise reduction in the room compared to an existing server room utilising in-room cooling.

Haas Ezzet, head of IT GLAM at the University of Oxford, contextualises this piece of work as being part of the "Museum's drive towards greater environmental sustainability. The approach piloted here, of focussing climate control specifically to the area needed, the data cabinet, rather than the entire space in which it is housed, will optimise energy consumption and afford a blueprint for other spaces within GLAM and beyond." ■

Ethernet needs more powerful testing

Christian Schillab, application engineer EMEA, Fluke

Ethernet is a flexible, yet complex networking technology which demands the use of efficient testing equipment and simplifies troubleshooting.

Since its introduction in the 1970s, Ethernet has displaced practically all other wired local-area network (LAN) technologies, because of its flexibility. Christian Schillab, Marketing Engineer at Fluke Networks describes why a flexible, yet complex networking technology demands a tester that keeps troubleshooting simple.

Flexible solutions for every application

Twisted-pair cabling coupled with the introduction of active hubs and switches made it possible for organisations to install Ethernet to support everything from multigigabit short-range links in the server room, to longer runs based on 100Base-T for connecting security cameras. The arrival of the IoT is making Ethernet increasingly important for building automation and other services that go beyond traditional IT.

To Power over Ethernet

At the electrical level, the four pairs of wires inside a typical Ethernet-grade cable such as the Category-5 (Cat5) provide a great deal of flexibility. The high-speed variants of Ethernet, such as 1Gb/s and 10Gb/s can use all four pairs to transmit data. The older and lower-bandwidth 10Base-T and 100Base-T versions use two of the pairs in the cable for data signals and the other two pairs for power.

A second mode combines data and power using electrical isolation circuitry. This makes it possible to use cables that have just two pairs of wires to supply power to 1Gb/s-capable devices. This is PoE's Mode A; Mode B employs the spare wires.

PoE can cope with sizeable power demands. In the case of Cat5 cable, the conductors are safe to carry as much as 360mA at 50V. In principle, a maximum of 36W can be delivered to a device at the other end from a power supply in the switch. In practice, the amount delivered will be lower as the electrical voltage drops with distance. A 100m cable might only be able to deliver 32W to the device at the far end. If Mode A needs to be used, the maximum power drops to just over 25W.

Safety Concerns

The PoE standard takes care of safety as well as compatibility issues through a negotiation process between the two devices at either end of the cable. First it detects whether a device able to receive power is connected by measuring the resistance across two wires. If it finds a valid resistance, it starts to negotiate what power is needed before activating the pairs that are needed. If it is wrong, it will not supply power.

The protocol is safe and effective. But it is clearly more complex than simply plugging a piece of equipment into a traditional wall socket. When things do not work as expected, the installer or maintenance technician is left with very few clues as to what is wrong. Is the cable broken or is it unable to deliver sufficient power to activate the device, perhaps because it does not have the requisite conductors? Is the switch failing to recognise a valid device or is the device itself at fault?

Effective troubleshooting

These issues are why access to effective cable testing equipment is vital in today's environment. Given the sheer variety of cabling and protocol options available for Ethernet, the technician cannot be expected to remember which combinations will work together. Their job is to make sure a security camera, lighting panel or a WiFi router is installed and can power up and work properly.

A common technique for attempting to test the performance of cabling links is to just use a pair of Ethernet transceivers in a tester and a remote unit and then attempt to connect, whilst communication can be tested, they do not actually measure the performance of the cable.

The LinkIQ provides the user with a gesture-based touchscreen that displays findings when plugged into an RJ45 port. It will perform electrical checks to determine if the cable connects to anything, and then runs tests to determine the performance of the cable in terms of its datarates, from 10Base-T to the gigabit-plus forms, as well as its ability to supply power. If cable is not connected at the far end, the technician can use remote ID units to find where it goes and why it is not connected to a switch port.

If there is a switch port at the other end, the LinkIQ will display statistics such as whether the switch has the capability to support the device being installed. For PoE, the unit can display the pairs where power is provided, including the different power levels and the wire pairs used. It will place a load on the connection to ensure that the advertised power is being delivered. As information on the network layout and performance is vital for maintenance, the unit can generate documentation after the tests.

Importance of simplifying testing

As Ethernet is now a complex, multifaceted networking technology with cabling that reaches into practically every part of wired infrastructure, technicians who deal with it need test equipment that can provide insights into its operation, inclusive of bitrates and connectivity, but also power. That is why a device such as the LinkIQ is now such an important tool. ■

Managing more connections

Joost Grillaert, product manager, Nexans Telecom & Data Systems

Bandwidth demand continues to grow which in turn leads to a vast increase in the number of connections. The question is how to manage this, given the fact that space in a data centre is limited and expensive. Simply stuffing all your racks with ultra-high density connections isn't recommended. So how then?

The drivers for this increase in bandwidth demand are tied to the rollout of 5G, IoT, the cloud, network convergence and more. For data centre operators, one of today's main challenges is to significantly increase the number of connections without using more space for rack units and cabling. After all, space for cabling and hardware in data centres is finite and generally limited. Partly because the space itself is expensive, but also because a great deal of available real estate is taken up by cooling and other facility equipment.

Higher density racks and patch panels make it possible to add significantly more connections in the same space. However, simply introducing the highest possible density throughout the data centre isn't the answer – partly for cost reasons but also from an access management point of view.

The most efficient approach is to install ultra-high density solutions where space is most restricted, and large volume connections are absolutely necessary. However in many areas in the data centre, where space is less of an issue, cost-effective lower density solutions are perfectly adequate. This approach can cover both fibre and copper requirements.

There are two main factors that determine density requirements: the size of the facility and the specific area in the data centre that needs to be connected. In a medium-sized data centre, for example, ultra-high density isn't always necessary. In large data centres, the number of connections required is significantly larger, and it might seem logical that there would be more space to accommodate these. However, the space in a large data centre is used up by servers and the amount of room available for patching isn't necessarily larger than in a mid-sized data centre.

In central patching zones, where hundreds of connections come together, and rack space is at a premium, with panels stacked on top of each other, it is definitely worth introducing ultra-high density patch panels. It is, however, essential to make sure that the choice of panel, cables and connectors allows easy (rear) access and moves, adds and changes can be easily and quickly carried out.

In server racks, however, fewer connections are required, and high density doesn't really bring any significant benefits. There's usually just one single panel at the top of the rack. Here, standard solutions offer more than enough connection capacity, although you need to ensure there's always some extra capacity for future expansions. Even if you only need 24 ports, we recommend putting in 48. Make sure you can reach the patch cords and cables from above or below.

Previously, there would always be a trade-off between introducing high densities and making operational aspects and procedures more difficult, but today's solutions balance these aspects better. For instance, for ultra-high density fibre patch panels the introduction of sliding trays greatly improve the accessibility to the patch cords and make it easier to patch in such dense zones. In addition, new generations of copper and fibre cords come with a significantly smaller diameter. They provide greater flexibility, support higher density, save space, introduce better airflow and less congestion, don't cause issues with sharp bends and ensure a nice and tidy look and feel.

It's important to realise that the number of connections required today in a given area of the data centre should remain similar for the next five to ten years. Although data requirements will continue to increase, this will be offset by higher bandwidth. Therefore, introducing very high density connectivity for future expansions in areas where you do not need those connections today might not be the right choice. You could be spending a great amount of money with a very uncertain future benefit.

When specifying a solution, the key questions are: can I get the right density at every location in my data centre? Can I support the needs for the core and access networks? Is patching still convenient? If in doubt, consult an expert!

PRODUCTS

The Future Plus Pre-term cabling System offers what the company reckons is one of the quickest and most reliable factory pre-terminated solutions. Each link is pre-terminated, pre-tested & pre-labelled before it leaves Future's facility in Oxfordshire. Available in Cat 5e, Cat 6, Cat 6a as well as LC, ST & SC fibre terminations.

Cat 6a - A solution for providing a 10 Gig installation, which makes the system "perfectly suited for communication rooms and data centre applications. "Future proofing today's cabling infrastructure is paramount and achievable using our Pre-term solution," the company says.

Cat 5e & Cat 6 – said to be ideal for all office, university or call centre applications, the four or six-way links provide a fully tested Gigabit solution to any workstation environment.

Whether laying cables to under floor boxes, wall outlets, and desktop pods or through false ceilings, "the system offers the best and fastest pre-terminated solutions on the market".

Fibre - installing a fibre backbone will future proof any new cabling infrastructure. The Pre-term Fibre Solution will allow the Installer to provide a 10Gig optical fibre link throughout the site with the choice of LC, ST or SC connectors. *futurend.co.uk*

The Excel solution provides cable to rack systems to suit data centre, hosting and co-location requirements of all types and sizes. A typical data centre installation has extensive requirements for seamless high-density design, high speed connectivity and infrastructure security. Excel offers a vast range of products, which, it says, "have been designed specifically with data centre spaces in mind", with choices across the copper, fibre, racks, power and containment product lines.

Excel reckons its comprehensive range of cable management solutions offer a variety of methods to route your cabling installations in the most appropriate directions and to manage the cables as and when required to maximise performance.

Excel also says it offers a host of products specifically to help with the installation and management of cabling components. The diverse range of cable management solutions are said to be compatible with the complete suite of Environ racks, cabinets and open frames, providing flexible options for both large and small data centre applications.

The selection of cable management solutions comprises of metal and plastic management bars and rings, vertical finger management units and trunk cable management solutions, among other products.

These solutions allow for the concise management of cables into the sides or the back of a rack, giving the same features and benefits of an open frame within an enclosed rack profile. *excel-networking.com*

Legrand, as the name suggests, is a French industrial group historically based in Limoges in the Limousin region. It was once the largest global producer of switches and sockets, with 20% of the global market and in cable management, generating 75% of its turnover internationally.

The Legrand Cablofil steel wire cable tray is supplied in straight lengths, "from which sophisticated installations can be created without the need for additional fittings". According to the company, the simply cut and shape lengths form bends, tees, crosspieces etc. and secure quickly and easily, using a range of 'slot and tab' fixings that do not require nuts and bolts.

In terms of its quality and durability, Legrand says its Cablofil steel wire cable tray has been tried and tested in installations of all sizes throughout the UK and beyond. Situations include flight duty requirements in small commercial buildings through to extra heavy duty installations in refineries and heavy industry applications such as shipbuilding. *Legrand.co.uk*

CommScope's premier copper and fibre structured cabling solution, SYSTIMAX, "provides the combination of power and high-bandwidth data connectivity and the flexibility to support advanced capabilities as you move to the ceiling". Born of innovation and backed by the strength and vision of a global leader, CommScope, SYSTIMAX's copper and fibre portfolio delivers, as it has for over 30 years.

Benefits of SYSTIMAX apparently include the bandwidth and power needed to make technologies like 5G, Wi-Fi and Wi-Fi 6E possible. The company also reckons the product supports all PoE standards and goes beyond overcoming application limitations in specific design configurations.

"To keep you ahead, we also offer our Application Assurance, a guarantee that specifications and performance will adapt and support your migration to higher-speed applications," CommScope says.

SYSTIMAX is also made to work with imVision: a unified approach to infrastructure management for unprecedented visibility and control over network connectivity. This software, combined with network controllers and accessories, allows you to locate and identify your equipment and ports as well as track any network changes. *commscope.com*

R&M has launched a universal Cat. 8.1 cabling system to support up to 40GbE. This system is backward-compatible as it's based on the standard RJ45 plug-in format. That means Cat. 6A patch cords used to date can still be deployed, while data centres and LAN operators don't need any additional adapters, transmission cables or fibre optic interfaces if they are later migrating to the faster network generations 25 and 40GbE.

After the installation of a basic Cat. 8.1 infrastructure, faster switches and servers can be integrated seamlessly. The basic Cat. 8.1 infrastructure consists of two RJ45 connection modules and a shielded Cat. 8.2/8.1 S/FTP installation cable. What's more, the system complies with both standard families: ISO/IEC 11801, Class I, and ANSI/TIA-568.2-D.

This system was designed for data centres (particularly with regards to top of rack and end of row cabling). Here, Cat. 8.1 cabling is due to transmit up to 40GbE in future, R&M says. It also guarantees the performance for the 24m permanent link and the up to 30m channel, depending on the patch cords used. *rdm.com*

Please meet...

Nick Dobrovolskiy, Parallels senior vice president of engineering and suppport

What was your big career break?

This would have been when I moved from being a developer to the CEO position at Parallels in 2003. At that time Parallels was a start-up and when I needed to run older OSes on newer PC hardware, I developed a solution which later became Parallels Desktop for Mac - a way to run Windows on Mac without rebooting. When Apple switched to Intel-based Mac computers in 2005, Parallels Desktop became famous virtually overnight.

One of my most memorable career moments was during a meeting with Apple to obtain approval for Parallels Desktop to join the Apple sales channel. Initially, some of the top execs were hesitant, then Steve Jobs joined the meeting and after firing some questions at me and my colleague, he simply said: "I think we should do it!"

Who was your hero when you were growing up?

When I was a kid, my hero was Bill Gates. When I was younger, I was always interested in computers and programming, which was something Bill Gates and I had in common. Like me, he wrote his first computer programme as a teenager and he went on to build the world's largest software company and now works for good causes around the world through his foundation. He is an inspiration.

If you could live anywhere, where would you choose?

It might not be an exciting answer when you think of all the amazing locations around the world where it's possible to live and work, but I'd have to say that I would always prefer to stay where I am based, in Moscow, Russia. It might not be Hawaii, Tokyo, Manhattan, Paris or Sydney, but Moscow is my hometown, it's where my family live and it is the place where I learnt to code and built my career. It was in Moscow that I got an early career boost when I won the Russian National Software Development Competition at the age of 14. That was a memorable day!

What would you do with £1m?

I find technology start-ups very exciting environments to work in, so if I had £1million I would love to become an Angel investor and invest my money into a few early product start-up companies. It would be great to be able to work with them and hopefully see them succeed and then know that I was able to make a difference.

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

If you're in the middle of a heated discussion, the best advice is to pause and think again, especially if you feel like all you really want to do is to reply to your opponent(s) with hard words. If you don't take this advice, you'll probably regret what you said later.

What's the strangest thing you've been asked?

Probably to jump out of a plane. It was not something I ever had a burning desire to do but once I did it, I caught the bug and have since become a certified skydiver. It's an unusual and exciting hobby!

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

I think I'd always work in technology but if I had to choose a different sector I'd probably be working in the automotive industry. This is because it's an extremely interesting area and has many similarities to software engineering. Vehicles can be almost like complex computers nowadays and I think I would enjoy the challenge.

The Beatles or the Rolling Stones?

Both are fantastic and legendary bands, but I am definitely more a fan of the Beatles, although I couldn't possibly tell you which is my favourite song as John and Paul wrote far too many great ones to choose from.

What's the one thing you must do before it's too late?

I don't really have a 'bucket-list' of things I feel I must do before I am no longer able. I am lucky because for me, the most important thing to do is something that I already do every day, and that is to kiss my wife and daughter, so they always know how much I love them. My family is the most important thing in the world to me and when I'm not working, I spend all the time I can with them.

What law would you most like to change?

I'm going to go with a slightly out of the box choice and say Newton's Law of Universal Gravitation. For those who aren't familiar with it, the law states that every physical mass attracts every other physical mass by a force acting along the line intersecting them. The force is proportional to the product of the two masses and inversely proportional to the square of the distance between them. Make sense?