

IN DEPTH: **DAS** - the future for indoor connectivity? p8-10



Beware the normalcy bias

Improving overall security efficacy

Trevor Collins, WatchGuard, p6



Is 5G the answer?

Security concerns must be realised

Tim Mercer, Vapour, p7



Questions & answers

'My father was my hero'

Neil McLoughlin, Nerdio, p16



Interserve faces £4.4 million fine for employee data breach



The UK's Information Commissioner's Office (ICO) has fined UK construction company Interserve £4.4 million following a sizable data breach.

Bad actors utilised phishing to gain access to personal data from 113,000 of Interserve's employees in 2020. National insurance numbers, bank account details, religion, ethnic origin, and sexual orientation comprised some of the data.

Interserve reportedly utilised outdated systems and protocols, neglected staff training, and had inadequate risk assessments. Its system failed to protect against the email phishing, leading to the compromise of 283 systems and 16 accounts; the company's antivirus system was uninstalled during the attack, and all employee information was encrypted.

"This data breach had the potential to cause real harm to Interserve's staff, as it left them vulnerable to the possibility of identity theft and financial fraud," said John Edwards, the UK information commissioner. "Leaving the door open to cyber attackers is never acceptable, especially when dealing with people's most sensitive information. The biggest cyber-risk businesses face is not from hackers outside of their company but from complacency within

their company."

The commissioner warned that companies that fail to monitor for suspicious activity, update their software, or provide proper training to staff will also be fined.

"If your business doesn't regularly monitor for suspicious activity in its systems and fails to act on warnings or doesn't update software and fails to provide training to staff, you can expect a similar fine from my office," warned Edwards.

ICO can impose fines of up to £17.5 million or 4% of global annual turnover but can reduce fines in case of mitigating arguments. In this case, ICO opted not to reduce the fine.

"The intention is to cause directors and chairmen to sit up and start asking questions of chief executives about cyber preparedness," explained Edwards.

Interserve has faced financial difficulties since 2017 and has undergone multiple financial restructurings before entering administration. In 2021, it resurrected the Tilbury Douglas brand for its construction and engineering businesses and separated from Interserve plc in June 2022. Interserve is expected to fully close in 2024. The years of financial challenges may point to why the company failed to invest in

new systems and protect employee data.

Commenting on the events surrounding the attack, Chris Vaughan, VP technical account management - EMEA & South Asia, Tanium, highlighted a worrying narrative.

"This incident follows a trend that I see when working with organisations to bolster their cybersecurity standards: too many still focus too much on reactive measures rather than preventative ones," said Vaughan. "A narrative has emerged across many IT teams that attacks are becoming too sophisticated to be stopped, and that therefore their efforts should be focused on reacting to security incidents rather than preventing them. However, I would encourage them to focus more on preventative measures which can either minimise the impact of breaches or avoid them altogether."

Sridhar Iyengar, MD for Zoho Europe, also commented: "businesses must have a clear understanding of how the third-party services they employ or partner with might be harvesting, selling or using their staff or customer data. This is a common tactic with many third-party tracker services for search engines, e-commerce sites and social platforms, and many businesses might not even be aware their data is being surveilled. ■"

DON'T GET YOUR SaaS KICKED!

TAKE CONTROL NOW

Protect your SaaS Data with **Arcserve SaaS Backup**

LEARN MORE →

Aberdeenshire to go smart with IoT

Aberdeenshire will benefit from a new Internet of Things (IoT) project which has the potential to transform the lives of those who live and work in the area.

Aberdeenshire Council will trial six smart technologies with North as part of its IoT Accelerator Pack Programme. The pilots will provide the council with access to real-time data insights on building health, social housing, water monitoring, waste management, air quality, and road surface temperature monitoring – allowing the council to make more informed decisions.

The Accelerator Packs are being rolled out to 12 towns across Aberdeenshire allowing the council to explore reductions across cost and energy consumption, while improving operational efficiencies and reducing carbon footprint, in support of the council's net zero commitments.

Five road temperature sensors will be installed across the region, increasing the council's ability to make more informed decisions, such as when to dispatch gritters, reducing emissions generated by extra trips, while smart waste management solutions will detect fill levels across a mix of fifty litter and grit bins to predict usage trends, allowing opportunities to identify more efficient collection routes and dates.

15 air quality sensors will measure

primary air pollutants, temperature, and humidity in real-time, so the council can determine trends across Aberdeenshire, which can be used to shape policy and decision making as well as improving health and wellbeing for those in the region. A number of the sensors will monitor air quality outside schools to determine the impact of vehicles when children are entering and leaving, while the council will also monitor the health of multiple schools across the council area, remotely measuring CO2 and humidity levels in place of current manual readings to improve efficiency.

13 Aberdeenshire Council tenants and one Sheltered Housing Scheme are also set to see benefits from intelligent housing technology which will give real-time insights into property health and condition, measuring temperature and humidity to proactively identify potential damp issues, allowing providers to fix any issues in advance, reducing maintenance costs and better supporting tenants.

Further sensors will be deployed across two schools and a care home to monitor water system conditions and water health, while ensuring ongoing compliance. The trial will allow potential efficiencies to be identified, such as reducing the need for employees to travel to check water outlets,



making better use of resources.

Using the results, trends and efficiencies from the trials, the council can create business cases for future investments and evaluate how they can digitally transform services to improve efficiency and effectiveness.

“Our Digital Strategy 2020 -2025 set out our priorities and commitments to optimising digital technology to improve our organisation, enable economic

growth, support the environment and benefit citizens and communities,” said Philip McKay, Project Sponsor at Aberdeenshire Council, said. “The North IoT Accelerator Packs presented us with the ideal opportunity to test and evaluate smart technologies that could potentially transform council services on a small scale, before committing to large scale investment. We are excited about the results these pilots could potentially deliver.” ■

World's largest offshore wind farm gains 4G

Vilicom has successfully deployed a Vodafone 4G mobile network for critical communications at the world's largest offshore wind farm in operation, Hornsea 2.55 miles off the Yorkshire coast.

The wind farm, which has just been completed by Ørsted, spans a 472km2 area in the North Sea. It consists of 165 8.4MW turbines which should generate a total power output of 1.4GW. It will be capable of powering over 1.4 million UK homes with clean electricity.

“At Vilicom we're delighted to play our part in a cleaner, greener future,” said Sean Keating, CEO of Vilicom. “The completion of this network is a huge achievement for Vilicom, Vodafone and Ørsted teams. Not only have we overcome the unique set of challenges involved in deploying a mobile network in the middle of the North Sea, but we have also accomplished this feat of engineering during a pandemic, with difficult operational circumstances.”

Vodafone and Vilicom teams worked for two years to build the communication infrastructure in tandem with the construction of the wind farm, which now supports a live Vodafone 4G mobile service across the entire wind farm. Ørsted's staff, all users, and vessels

can now seamlessly enjoy the same reliable network experience as they do onshore.

Vilicom has built and will power the critical communications infrastructure to enable workers to access the data and information systems needed for the operation of the wind farm, as well as giving them the ability to stay connected with family and friends using their personal devices.

During the construction phase, Vilicom also delivered a temporary solution to provide connectivity to the employees working across a five-vessel fleet of floating offices. The wind farm will support opportunities for economic growth, contributing to the UK's goal for renewable electricity generation.

“It is so important to have a 4G network that allows us to improve the efficiency of construction and operations of the world's largest offshore wind farm,” said Patrick Harnett, vice president UK programme, Ørsted. “It's also very important for our colleagues working out at sea to be able to connect back home to their friends and families. The wind farm which has become fully operational in August this year, will have the capacity to provide the UK with clean, green energy for 1.4 million homes.” ■



WiFi 7 named key emerging area for investment

According to the Wireless Broadband Alliance (WBA), WiFi 7 is emerging as one of the most important areas of investment in new connectivity technologies.

The findings, released as part of the WBA Annual Industry Report 2023, reveal more than a third of service providers, technology vendors and enterprises have plans to deploy WiFi 7 by the end of 2023. WiFi 7 will supercharge current WiFi capabilities with new technologies, such as multilink operation and time sensitive networking - ideal for Industry 4.0 applications - while leveraging the 6GHz spectrum dynamically with automatic frequency coordination.

The report also revealed that WiFi 6E has now become the de facto industry standard, with 53% having already deployed the technology and a further 44% already working on plans to adopt WiFi 6E in the next 12-18 months.

Uptake of WiFi 6E and WiFi 7 is being driven by a growing appetite for data-intensive, low-latency applications and use cases, from smart cities and immersive technologies such as the future metaverse to Industry 4.0. Newer WiFi technologies offer better scheduling and greater interference management, which survey respondents now see as essential in supporting high-quality video, virtual reality (VR), augmented reality (AR) and other advanced consumer experiences.

The report detailed a renewed focus on the quality of experience (QoE) delivered to end-users, with 90% of service providers, equipment manufacturers and enterprises

now ranking it as a key differentiator in monetizing their WiFi services. 61% percent of respondents identified services such as high-definition video streaming, AR, VR and potential metaverse applications as key revenue opportunities.

Other key findings from the report reinforce the need for convergence between WiFi and cellular technologies in the interests of creating a seamless user experience. In enterprise markets, 70% said WiFi and 5G will coexist, with 61% claiming convergence would support enhanced flexibility for enterprise services. 53% said that convergence between licensed and unlicensed technologies was critical or important for the current commercial strategy.

“What we're seeing here is the industry at large identifying increasing value in WiFi technology in the wake of highly anticipated new use cases. What's more, service providers, equipment manufacturers and enterprises around the world know that those use cases are best served in a converged environment, where WiFi and 5G complement each other,” said Tiago Rodrigues, CEO, WBA. “Therefore, we're seeing the industry advance at breakneck pace toward WiFi 7, with mobile operators leveraging WiFi as part of their 5G strategies to maximize coverage and optimize capacity – it's all about the user experience. This includes how people and things connect to the networks - automatically, securely and with privacy assured and that is where OpenRoaming provides the essential ingredient.” ■

EDITORIAL:

Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Robert Shepherd, Abirami A, Nathan Howe, Kyle Davies, Scott Davis, Mark Garner, Mark Wharton, Chris Berry, Knud Kegel, John Hall, David Sanders, Matt Edgley, Eric Herzog, Simon Brady and Richard Clifford

ADVERTISING & PRODUCTION:

Sales: Kathy Moynihan
kathym@kadiumpublishing.com

Production: Karen Bailey
karenb@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

© 2022 Kadium Ltd. 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

Sustainability lacking in IT and DC operations

Schneider Electric has commissioned two independent research studies focused on sustainability in IT and data centre operations - the results reveal a disconnect between intent and action, indicating most of the industry is still at the beginning stage of its sustainability journey.

The two studies were conducted by 451 Research and Forrester. They collected data from nearly 3,000 global participants, including the largest colocation and cloud providers, and IT professionals across many segments and organisation sizes. The 451 Research paper revealed a perception-versus-reality dilemma with many enterprise organisations believing their sustainability programs are more advanced than they are, as "the maturity evaluations of nearly half of respondents (48%) did not match a previous

answer." The Forrester paper focused on colocation and found 73% of organisations ranked sustainability as their #2 business priority, but only 33% say they have created a strategic sustainability plan.

"The research clearly demonstrates that across the data centre and IT industry, there is a sustainability action gap - the intention appears to be there, but action is lacking," said Pankaj Sharma, EVP of the secure power division, Schneider Electric. "Of course, IT professionals understand and have taken steps to address sustainability. But what we lack, with some exception, is comprehensive and supported sustainability action plans and measurable targets to create the change required to address the climate crisis. These two research papers have documented a sustainability action gap and that is our

collective challenge to address.

The 451 Research White Paper researched more than 1,150 medium and large enterprises worldwide representing more than 20 verticals and their sustainability efforts with distributed IT resources. Researchers found that many enterprises believe they are further along in their sustainability journey than they actually are. For this group, the main driver of sustainability is business value and firms start with measuring energy usage then expand into other sustainability metrics and tools. The greatest challenges in their sustainability journeys include optimising energy usage, followed by obtaining consistent data and metrics (for leaders/advanced firms) and lacking skilled staff (for starter organisations).

The leadership paper from Forrester polled 1,033 global sustainability decision-makers

at colocation providers worldwide with the objective of exploring sustainability drivers in the colocation provider industry. The study also explored the major challenges for colocation players and where they are investing the most across the technology stack. The paper found organisations lack a strong comprehensive strategy for the sustainability programs, with only 33% saying their business has created a strategic sustainability plan, indicating that the industry is still at the beginning of a sustainability journey. The paper determined that moving forward, a key piece of sustainability success will be finding the right partner to help organisations succeed. It also found that businesses that hired an outside sustainability consulting firm as part of their sustainability initiatives are 33% more likely to be high maturity. ■

Cloud telephony provisioning automated

Callroute has partnered with Coolwave Communication to automate the provisioning of cloud telephony services across UCaaS and CCaaS platforms. Enterprises can easily connect Coolwave's global SIP trunking to Microsoft Teams and Webex without requiring physical infrastructure or extensive technical knowledge.

Voxnube is the first to unlock the benefits of this partnership. The company provides distributor voice services and solutions to Callroute and Coolwave's partner bases globally, while benefitting from Callroute's advanced call routing, number management and user provisioning solution, coupled with Coolwave's extensive SIP trunking capabilities.

"Coolwave is very excited to be supporting Callroute in delivering global SIP solutions. Callroute has developed an advanced call routing, number management and user provisioning solution, allowing you to connect any phone system and service provider together, without the need for infrastructure or deep technical knowledge," said Ronan Higgins, commercial director at Coolwave Communications. "Together, we are making it simple for all kinds of businesses to optimise and grow their UCaaS, CCaaS and CPaaS platforms with BYOC and automated voice services, helping to accelerate their services for customers."

Using Callroute, end customers can easily connect Coolwave's global SIP network to UCaaS platforms such as Microsoft Teams using the Callroute Bring Your Own Carrier (BYOC) functionality. In combination with Coolwave's cloud-based, self-service and white-label Cool Operator platform, partners and customers benefit from secure and superior voice quality with regionalised points of presence, which simplifies global telephony deployments. ■



printserver ONE - the optimised Print Server for a secure network

A network printer usually has an interface and an additional USB port. In some network configurations it may be necessary to operate more than one network interface on a printer. This is where the printserver ONE comes into play - simply connect it to the USB interface and the second interface is available! Printed matter is received fully encrypted and forwarded to the printer. Hacker attacks can be prevented even on devices with an Internet connection!

Your Benefits

- ✓ Powerful throughput rates
- ✓ Encryption of print data
- ✓ Equip printing systems with 2nd network interface
- ✓ Simple user interface, time-saving installation and administration, monitoring and maintenance via browser
- ✓ Comprehensive security package including encryption, current authentication methods, access control and many more
- ✓ Operate separate private and public networks using secure printing over an IPSec connection
- ✓ Up to 60 months free guarantee
- ✓ Regular updates and free technical support worldwide



printserver ONE



For All Printing Systems That Feature a USB Port

Ink-jet printer, laser printers, label printers, large format printers, plotter, dot matrix printers, barcode printers, multi-function devices, digital copying machines and many more!



SEH - 35 years of innovative product development

SEH Technology UK Ltd.
The Success Innovation Centre,
Science Park Square,
Falmer-Brighton, Great Britain,
BN1 9SB

Phone +44 (0) 1273-2346-81
Support +49 (0) 5 21 9 42 26-44
Internet www.seh-technology.com/uk
E-Mail info@seh-technology.co.uk

■ Made in Germany

You're responsible for the protection of your SaaS Application Data. Did you know that?

SaaS vendors own the cloud infrastructure stack and all primary components that make up the service such as physical infrastructure, network controls, the operating system that hosts the application, controls for the application offered as a service, hardware components, and more.

But data—the critical component that powers your business and is central to the service's relevance—is your organisation's responsibility.

This is because SaaS vendors operate on a shared responsibility model, which means obligations are shared between the vendor and the customer.

Data is your most important asset

In today's digital economy, data has become the currency of enterprises. Losing it will result in potential loss of customers, brand, revenue and ultimately the company.

In a study conducted by ESG, 81% of Microsoft Office 365 users had to recover data, but only 15% were able to recover 100% of their data.1

Complete Protection for SaaS Data

Cloud data protection is your responsibility. And moving data to the cloud exposes it to risks. Having a comprehensive solution to protect data hosted in SaaS applications is the only right move for any organisation.

Arcserve SaaS Backup offers complete protection for data stored in Microsoft 365, Microsoft 365 Azure AD, Microsoft Dynamics 365, Salesforce, and Google Workspace.

Conclusion

SaaS vendors have made it clear that backups are the organisation's responsibility and not theirs. Arcserve SaaS Backup adds to Arcserve's powerful portfolio, equipping organizations to completely protect their SaaS data, eliminating business interruptions due to unrecoverable data loss.

Download our eBook, "Top 5 reasons why you need SaaS Data Backup", to learn more, and protect you SaaS today!

1Source: ESG Technical Validation, Keepit: Dedicated Data Protection For SaaS Workloads. Delivering Data Availability, Cost-Efficiency, Simplicity, Instant Recovery, And Total Security by Dolan, Kerry, Sr. IT Validation Analyst. October 2021.

Data protection emergency

Veeam Software has reported that UK and Irish businesses are headed for a data protection emergency.

Nearly eight in ten (79%) of UK IT decision makers and professionals disclosed gaps between their data dependency, backup frequency, SLAs and ability to get back to productive business when asked by researchers compiling the Veeam Data Protection Trends Report 2022.

Meanwhile, 76% of respondents admitted falling prey to at least one ransomware attack in the past year, with 65% now using cloud services as part of their data protection strategy to increase resiliency. 20% of IT leaders polled say they will change backup solutions for cost reasons, while 23% are

looking to improve results.

Despite this, businesses are losing the battle when it comes to defending against ransomware. 88% of ransomware attacks attempted to infect backup repositories to disable victims' abilities to recover without paying the ransom, 75% of those attempts being successful. One in three organisations say that most or all their backup repositories have been impacted as part of a ransomware attack.

While companies report that 47% of data centre servers, 50% of remote offices and 44% of cloud instances are impacted in an attack, paying the ransom is not a recovery strategy. 29% of organisations who paid the ransom could not recover their data. ■

Bus shelters gain 4G with small cells

Freshwave and Clear Channel UK have devised a solution to allow 4G mobile small cell technology to be integrated into bus shelters in Tower Hamlets, London.

As a result, small cell technology - from any infrastructure-as-a-service provider - can be installed anywhere with a Clear Channel shelter and a requirement to increase network capacity in the area. Following the success of this new approach, the 5G-ready technology will be added to further bus shelters in the borough in the coming months.

Busy areas such as high streets, where bus shelters are already providing an essential public service, place greater demand on networks as more people are trying to use the mobile signal from the same macrocell. Outdoor small cells immediately increase access to top speeds and capacity in the area around them, making it easier for people to connect. Using existing street assets, as opposed to building new assets, not only makes it faster and easier for the mobile operators to enhance their networks, it also reduces the

amount of clutter on the streets.

"I'm proud of our constant engineering and design innovations, as well as the way we collaborate in new ways with industry partners and local authorities. Smart cities and towns need new approaches to digital connectivity," said Simon Frumkin, CEO at Freshwave. "And the more existing street assets that can be used to bring this to our towns, the better it is for both the mobile network operators and the customers and communities they serve. This is why we're already working on a multi-operator, multi-technology design for bus shelter use too." ■



World Quality Report highlights green IT

The 14th edition of the World Quality Report, which examines the key trends and developments in Quality Engineering and Testing (QE&T), highlights sustainable IT and value stream management as new interest areas for quality teams.

Research revealed that while the role of quality within sustainable IT is still evolving, 72% of organizations think that QE&T could contribute to the environmental aspect of sustainable IT. Respondents are also optimistic about the benefits of green engineering as part of their sustainable IT strategies, with 47% of respondents citing improved brand

value ranking as the most important benefit, followed closely by improved customer loyalty (46%).

While awareness is growing on how quality strategy can offset various risks associated with deploying new technology, the quality assurance function is transforming at speed from pure testing to actual quality engineering practices. For example, 88% of respondents agreed they were at medium to high risk of losing market share to a competitor and 90% agreed that they face risk of increased costs for the deployment of new technology solutions without a QE&T strategy. ■

Gov gains fully managed data networks

Arqit Quantum Inc. and Nine23 Ltd will deploy Arqit's QuantumCloud™, a symmetric key agreement software, on Nine23's UK Sovereign Secure Private Cloud infrastructure. The partnership will deliver a fully managed UK sovereign deployment of QuantumCloud™ for government and defence customers across data networks and infrastructure without the need for significant changes to the existing hardware, software, or support. ■

2022's biggest cyber threats named

OpenText Security Solutions has announced the Nastiest Malware of 2022, a ranking of the year's biggest cyber threats.

The 2022 'Nastiest Malware' were named as: Emotet, LockBit, Conti, Qbot (AKA Qakbot), Valyria, and Cobalt Strike and Brute Ratel.

For the fifth year running, OpenText's threat intelligence experts combed through the data, analysed different behaviours, and determined which malicious payloads are the nastiest. Emotet regained its place at the top, reminding the world its masterminds are resilient. Analysis also revealed an almost 1,100% increase in phishing during the first four months of 2022 compared to the same period in 2021, indicating a possible end to the 'hacker holiday,' a hacker rest period following the busy holiday season.

"The key takeaway from this year's findings is that malware remains centre stage in the threats posed towards individuals, businesses, and governments," said Muhi Majzoub, EVP and chief product officer, OpenText. "Cybercriminals continue to evolve their tactics, leaving the infosec community in a constant state of catch-up. With the mainstream adoption of ransomware payloads and cryptocurrency facilitating payments, the battle will continue. No person, no business - regardless of size - is immune to these threats." ■

Vertiv targets data centre sustainability

Vertiv has launched the Guide to Data Centre Sustainability, an online resource for data centre owners and operators seeking to reduce their environmental impact.

According to the International Energy Agency, data centres account for about 1% of global electricity demand. The industry has limited the impact of capacity growth on energy consumption prior to 2020 by improving operating efficiency. However, in 2020, internet traffic exploded by more than 40%, and market intelligence projects a 13% compound annual growth rate (CAGR) in data centre construction over the next five years. With increased focus on reducing greenhouse gas emissions and water consumption, operators are seeking new solutions to increase equipment utilisation and drive out remaining inefficiencies, phase out water-intensive cooling technologies, and decrease dependence on carbon-based energy sources. ■

Word on the web...

IT optimisation: reducing costs and increasing efficiency

Alan Hayward, sales & marketing manager, SEH Technology UK Ltd

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





Five key steps to defend your organisation from harmful phishing attacks

Chris Watkins, head of security, Ultima

Some of the worst cybercrimes have taken place because of a tiny flaw. Cybercriminals rely on this flaw in an organisation's security defences – commonly the employees themselves – to launch their attack. You only need to look at the number and scale of phishing attacks taking place every year. In 2021, 83% of organisations reported experiencing phishing attacks. In 2022, an additional six billion attacks are expected to occur.

Many phishing defences start and end with employee training to help them spot a phishing email. Empowering employees is certainly a key strategy. But employee education is only a part of the solution. Organisations can widen their defences using technical measures as well as reporting processes and plan for attacks to minimise their impact.

Phishing at its worst

A phishing attack is where a malicious hacker launches an email-based attack with the objective of obtaining user credentials so that they can gain a foothold within a corporate network and use that foothold to exploit data or demand a ransom. Cybercriminals use deception tactics to encourage users to click on a link which launches malware or makes the user give away details such as usernames, email addresses or better still, passwords.

Phishing emails are so common because it's a numbers game; if a phishing campaign circulates to enough users (often in the millions), it increases the chance of success. Such data breaches not only cause loss of company data but lead to loss of revenue from a decline in customer trust and market value.

Here are five steps to take to bolster the defence of your corporate network that should be combined with effective employee training.

1. Review how you're preventing phishing emails reaching you in the first place

Whether manual or through your cloud-based email provider, ensure that the filtering or blocking service is sufficient for your needs and that it is applied to all users' accounts. A filtering service will send them to a junk folder, whereas a blocking service will prevent the email getting through to the user completely. This is based on the senders IP

address, domain name, attachment type or because it's detected malware.

2. Think like a hacker

Often, thinking like a hacker is the best way to spot one and this involves gaining an understanding of the nature of the threat that phishing poses to your organisation. What would a hacker want from an employee? Which departments are managing processes that are most sensitive (such as product development or finance) and could these processes be mimicked by a hacker?

3. Make specific processes more resilient

This involves good cyber hygiene practice. If dealing with many external email requests, try using multi-factor authentication, such as an SMS message or phone call to verify the sender. Rather than sending and receiving email attachments, use a different login method or share files through an access-controlled account in the cloud such as Dropbox or Microsoft Teams.

4. Adopt a zero-tolerance security culture

It's important to be realistic – not everyone

can spot a phishing email 100% of the time. Phishing emails have become much more sophisticated in recent years.

Zero trust is the mindset of 'protect everyone, verify everything.' Every user and device accessing a network is a potential threat. A zero-trust policy requires employees to act with a healthy dose of scepticism to everything that lands in their inbox. Such a culture brings the employee into the broader security network, establishing trust between the organisation and employee while increasing resilience.

5. Encourage transparency and ensure ease of reporting

Often, it's the phishing culture within an organisation that needs to be improved. Far from pointing the finger and assigning blame to an employee, it's important to foster a culture of awareness, support, and action. If an employee feels that they are going to be reprimanded for not spotting a phishing email or making a mistake, they may not report it promptly, or at all.

Implement a process that is easy to follow when an employee believes that a phishing email has made it past the company's technical defences. Once it's been reported, make sure that employees know that it will be actioned so that they feel encouraged

to repeat the exercise again. Create an environment where employees aren't afraid to ask out loud for extra support in spotting phishing attacks.

Being involved in an organisation's awareness and reporting culture should all form part of an employee's wider security hygiene which also includes password management, use of removable media and remote working practices among other things. As an organisation, this should be actively encouraged to ensure that security is maintained.

In summary

A combination of education, simulation, transparency and effective security reporting, along with leading-edge security tools are necessary to create a zero-trust organisation. From a technology perspective, this could involve multi-factor authentication, a VPN, encryption for files and updated hardware. Together, they can create a more secure corporate environment for all.

The reality is that there are always going to be threats that creep into a company's layers of security. But if an organisation has the necessary security technology, employee education and a strong culture of zero-trust, then identifying and reporting threats becomes innate in everyone. ■



A flexible UPS that fits your needs

Collaborate IT

Vertiv Platinum Solutions Provider

Vertiv™ Edge UPS

500 – 3000 VA 230V

Superior Power Protection for:

- Edge Applications
- IT Servers
- Network Equipment
- Telephony
- Storage
- Security Systems



COLOR LCD display

0.9 PF High output power factor (0.9)

Controllable outlets

Efficiency up to 98%

Rack/Tower flexibility

In stock

Is it time to rethink your power outage protection?

W: www.collaborate-it.com T: +44 (0) 203 889 8458 E: sales@collaborate-it.com

Rack | UPS | Cooling | PDU | Access | Monitor | Service | Support

Beware the normalcy bias



Trevor Collins, security analyst, WatchGuard

Protecting our corporate networks by implementing security best practices and policies is critically important and it can take months to set up the proper security solutions to help meet these goals. But even after all that, some organisations still experience breaches from simple user mistakes, while security professionals often miss an important element of security – mitigating normalcy bias.

What is normalcy bias? It is a cognitive bias that leads people to disbelieve or minimise threat warnings. Consequently, individuals underestimate the likelihood and impact of a disaster that might affect them. This is extremely applicable when thinking about cybersecurity and users. How do you balance a user base that includes those that prepare for the worst-case scenario and those that don't? So-called 'preppers' often overestimate the likelihood of an apocalyptic event and suffer from worse case thinking bias. But non-preppers too easily dismiss the need to prepare for a breach. This is normalcy bias and can have a heavy impact on the execution of employee best practices.

While users often understand the likelihood of a security incident happening, they fail to see how their actions might cause one. They don't intend to help cause a breach, but normalcy bias allows them to believe that the actions they take won't contribute to a negative security event. Normalcy bias also leaves users with the belief that if an event does occur, it won't cause much damage.

The reality is that users base their actions on how often they see and experience something, instead of how often something happens. This 'user error' is a big contributing factor in security breaches and can be the result of excessive warnings that lead users to ignore them. For example, when's the last time you read a medication warning on a packet of paracetamol or noticed the warnings in a petrol station?

Shifting this to organisational security; how often do you accept the updated Facebook privacy policy without reading it or take notice of the advice from your bank around spoof emails? The sheer number of warnings users encounter daily leads many to automatically diminish the severity of the next one. The threat becomes normalised. These excessive warnings often come from a focus on protecting the creator of the warning from being held responsible, instead of helping the user avoid pitfalls.

So, how does an organisation work to overcome normalcy bias to improve overall security efficacy within its user base? There are two key elements: education and training, and security solutions. When it comes to the human element of normalcy bias, here are three tips to consider:

1. When creating security policies, we must not prevent productivity. For example, policies that block users from changing

the desktop background tend to hinder productivity and create a disconnect between the user and the company, thus increasing normalcy bias. We also can't dismiss the end goal of company growth in the name of cybersecurity. If we prevent growth, then we aren't helping anyone.

2. Conduct regular training – at least quarterly – that focuses on the users' ability to prevent the latest threats facing the organisation and the impact of user error. Embed a security-first mindset into the corporate culture starting from the top. Offer users educational materials that allow them to understand the problem and the role they play. Share real-world examples and encourage users to do the same. Ensure leadership is setting good examples and advocating best practices. Inform users of their own importance in keeping the company secure. No one likes to admit they've made a security mistake. That's why organisations need to encourage users to report errors they see or make. And once an error has happened, there needs to be follow-up with the user to ensure they understand the problem and know how to avoid it moving forward.

3. In many IT and development environments, employees have tight deadlines to complete projects. From the perspective of the user, they must complete the project in the timeline provided. They also need to balance the project with security protocols and if not given enough time, security is often the element bypassed. Regardless of job function, organisations need to build in the proper amount of time for security policies and technologies to be used. This often means that managers and team leaders need to be informed of the impact of security policies and account for security training for their teams.

Normalcy bias is often just chalked up to the need for better training, and while that is critical, it's much deeper than that. Warnings should be designed to help the user, not just to protect the provider or vendor from liability. Eliminating normalcy bias means making a cultural shift within the organisation that allows users to be the solution instead of the problem. This means making them an active part of the security strategy and arming them with best practices, education and training, so they can work to proactively help protect their organisation.

Organisations may feel the urge to provide warnings on every point of danger, but this diminishes the bigger problems. Users and security have a complex relationship along with the human element involved, and mitigating normalcy bias is just one element in an organisation's overall security strategy. By talking about it, the security community can work together to help better address the challenges it presents. ■

DATA centres Ireland

16-17 Nov 2022
RDS, Dublin

Platinum Sponsor



Strategy Stream Sponsor



Infrastructure • Services • Solutions

DataCentres Ireland combines a dedicated exhibition and multi-streamed conference to address every aspect of planning, designing and operating your Datacentre, Server/Comms room and Digital storage solution – Whether internally, outsourced or in the Cloud.

DataCentres Ireland is the largest and most complete event in the country. It is where you will meet the key decision makers as well as those directly involved in the day to day operations.

EVENT HIGHLIGHTS INCLUDE:

Multi Stream Conference • 25 Hours of Conference Content • International & Local Experts • 60 Speakers & Panellists • 100 Exhibitors • Networking Reception

Entry to ALL aspects of DataCentres Ireland is FREE

- Market Overview
- Power Sessions
- Connectivity
- Regional Developments
- Open Compute Project
- Heat Networks and the Data Centre
- Renewable Energy
- Standby Generation
- Updating Legacy Data Centres

Supporting Organisations



Meet your market

For the latest information & to register online visit www.datacentres-ireland.com



KVM CHOICE

Total Control in Computing



Specialist suppliers of Datacentre equipment call for a quote today!

See our latest 'working from home solutions'

HASSLE FREE PROCUREMENT OF: IT / POWER / INFRASTRUCTURE EQUIPMENT



sales@kvmchoice.com | sales@pduchoice.com
www.kvmchoice.com | 0345 899 5010



Unleash the
security of

ONE



NETWORK
SECURITY



MULTI-FACTOR
AUTHENTICATION



SECURE
CLOUD WI-FI



ENDPOINT
SECURITY

Smart Security, Simply Done.



Saving lives with DAS

Poor in-building connectivity isn't something you consider until it happens to you, and while it may be frustrating for consumers, it can be truly business or even life-threatening for private and public enterprises. Amy Saunders explores how distributed antenna systems are solving indoor connectivity challenges

Connectivity has moved on from being a nice-to-have to playing an essential role in the modern world. Enterprise, government, business and consumers alike have come to rely on ubiquitous, always-on connectivity to go about their daily lives.

In the 21st Century, we spend more time inside than ever before; work (on-site, off-site or from home), leisure, shopping, socialisation, etc. are more often than not based indoors. In the UK, the average person spends 22 hours of their day inside – that's 90% of their time. With so many aspects of day-to-day life now relying on connectivity, having access to high-quality, seamless solutions while indoors is essential.

The challenge of indoor connectivity has never been more pressing. With the

advent of the COVID-19 pandemic, and the 'stay home, save lives, protect the NHS' message, suddenly we were faced with even more time indoors. This only served to highlight the numerous in-building connectivity blackspots nationwide.

The trouble with blackspots

Blackspots have been a challenge since the advent of wireless communications. Rural and remote locations naturally have issues with connectivity if the closest cell tower is just too far away; however, blackspots are also a problem in urban environments.

Signals travel best through free space – the lower the frequency, the better the transmission through solid materials, although distance from the source is also a factor – any physical objects in the way

have the potential to cause disruptions. Such disruptors include buildings, tunnels, corridors, and certainly underground networks. Certain buildings are more prone to blackspots than others, like hospitals: thick walls, safety glass, elevators, basements, and hundreds/thousands of private rooms, each with their own four walls, don't make for great conduction. Many government buildings and corporate offices with the same makeup suffer similar poor signal availability.

"The need for cellular connectivity will not only become more necessary, but also more of a challenge. Construction materials used to make a building more environmentally friendly cause havoc with cellular signals," said Stephen Kowal, Nextivity CCO.

The changing environment and moves

towards increased digitisation, with IoT and M2M playing a key role going forwards, are also putting pressure on indoor connectivity.

"There are several challenges associated with indoor connectivity," said Markus Nispel, EMEA CTO, Extreme Networks. "These range from the exponential increase of connected devices driven by IoT, BYOD and digital transformation in general to higher bandwidth demands and experience expectations from users and applications. All this needs to be considered when planning and operating indoor networks."

"As our dependency grows on our mobile devices, the need for connectivity inside of buildings will also grow," said Kowal. "Additionally, the need for machine-to-machine communication



will drive growth for low power, high resiliency cellular connectivity. It is our belief that all companies will need a complete wireless strategy that includes WiFi, public cellular, private cellular, and IoT connectivity.”

In the UK, Statista reported that indoor coverage for 4G in 2019 hovered around 92.5%, with three of the nation’s four providers all covering more than 90% of locations: O2 at 95%, Vodafone at 94%, EE at 92%, and Three at 89%. O2 and Vodafone broadcast their 2G/3G signals at 900MHz, which is better for penetrating indoor environments, while EE and Three operate at 1800Hz and 2100Hz, respectively; the higher frequency waves do not travel so well through solid materials.

Around 80% of mobile calls originate indoors, so it can be frustrating to discover that you’re working or living in a blackspot. It’s been reported that working in a blackspot can reduce business productivity and cause such annoyance that one in four staff would consider quitting.

There are several different solutions for solving indoor connectivity blackspots, however, according to CommScope, just 2% of the world’s 30 billion square metres of office space is covered by in-building mobile wireless systems.

Delivering indoor connectivity

While femtocells and repeaters/boosters/extenders provide one solution to meet indoor connectivity challenges, larger, more scalable systems are better suited for enterprise applications. Indeed, for enterprise users, heavy duty solutions are required to ensure always-available, high-quality connectivity.

Small cell systems are one such solution, featuring a low-cost radio access point with low frequency power output, small footprint, but limited range. Suitable for indoor or outdoor use and supporting one or two frequencies, each individual node requires its own power supply and operates independently of other nodes, supporting up to 25 users. These are ideal for improving coverage, adding targeted capacity, and supporting new devices and user experiences. However, they are less versatile than distributed antenna systems (DAS), which can support several frequencies simultaneously for multiple

carriers, and can support almost 2,000 users with just one backhaul pipe.

Indeed, DAS has really made its mark on the enterprise world in recent years. Such systems are convergent unified signal transmission mediums which connect separated antennas to provide wireless signals indoors. Multiple signals supporting both voice and data are supported via a single cable.

DAS can operate in multiple frequency bands simultaneously, while supporting different technologies and providers. High-quality mobile data networks can be delivered to venues of all types – hospitals, stadiums, airports, offices, government buildings, etc. – and support different communications protocols, while remaining relatively maintenance free. Such systems are easily and cost-effectively scaled to augment coverage, and spectral efficiency is improved, reducing interference.

“The main advantage of DAS is that it can handle very big, complex environments, like 70-storey buildings, arenas, stadiums, hospitals and travel hubs,” said Brendan Hourihane, senior director enterprise and real estate, Freshwave. “From an in-

building perspective, often you only need to deploy one radio on, and sometimes above, the ceiling. So that means less kit to buy and install and it can also be easier from an aesthetic point of view which is important in premium commercial buildings. However, in high-capacity areas you may need multiple radios should you need to deploy multiple-input multiple-output technology (which depends on the MNOs).”

Saving lives with DAS

The COVID-19 pandemic brought to light a great many problems within networks across the UK.

During the pandemic, warehouses and conference centres were converted into emergency facilities within weeks to aid national efforts. Reliable, ubiquitous mobile connectivity was central in their smooth running, with voice and data services essential for admissions, internal and external communications, supply management, etc. Additionally, in a world with social distancing and isolation rules, indoor connectivity replaced in-person visitors for patients. WiFi was not

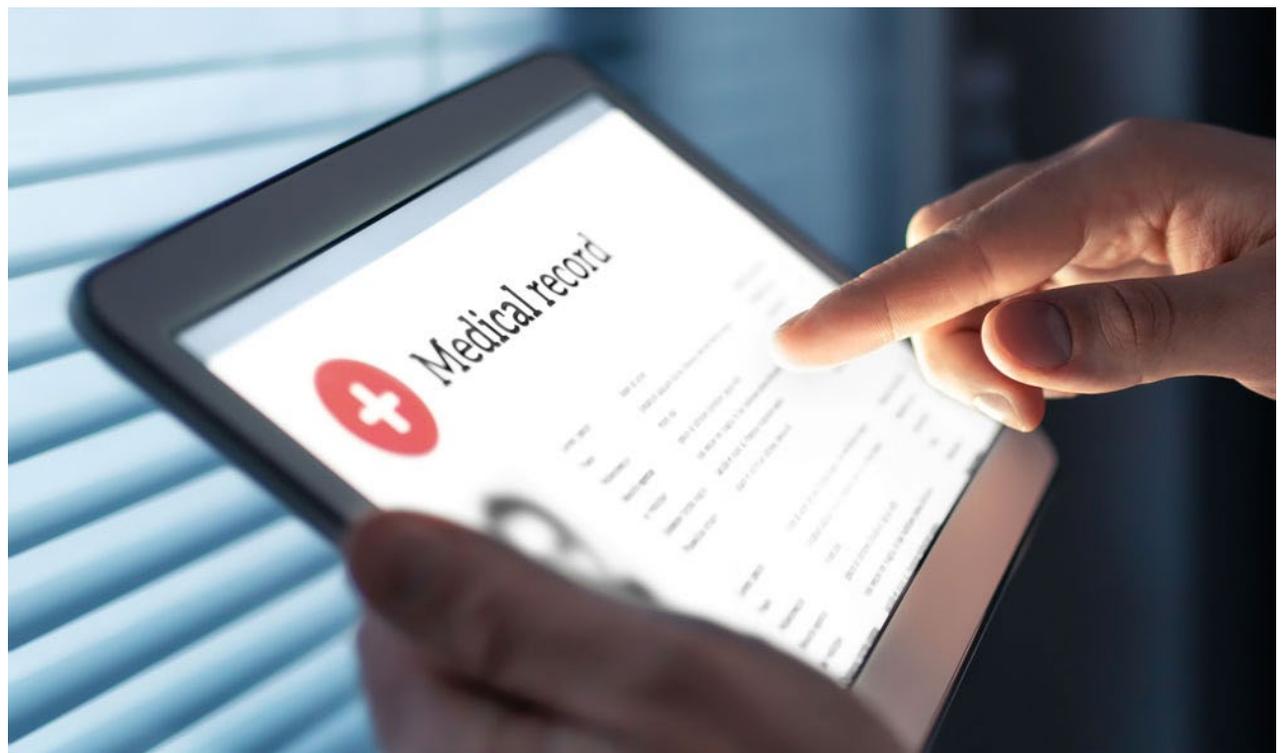
stable or secure enough to rely on within many buildings, with quality-of-service (QoS) issues posing a risk to patient wellbeing. While the UK’s four MNOs banded together to augment capacity, this did not translate into automatically better coverage due to indoor signal transmissions challenges.

A significant number of NHS hospitals have chosen to install DAS to provide reliable connectivity for both staff and patients, some in the midst of COVID-19, to ensure that: digital patient records on tablets and mobile phones were accessible; staff were able to communicate effectively; organisation and planning (mobile devices are increasingly being used to plan rotas and for patient visits; and patients could speak with their next of kin).

One such example is Central Middlesex Hospital, which suffered with patchy or non-existent coverage at several of its buildings, and which became even more problematic during the pandemic. The Central Middlesex Hospital building covered a 36,500 square metre area over three floors and was fitted with a hybrid QUATRA signal booster and passive DAS solution with twelve systems in total to balance coverage, performance and cost. The hospital now has full mobile coverage in the required areas to support clinicians and patients. The solution is monitored and supported via a managed service from Cision and UCtel, ensuring that coverage is maintained and any incidents or changes in the environment are quickly addressed.

Perth Royal Infirmary has a similar story. Having struggled with poor mobile signal for years, an upgrade was required to improve connectivity and mobile coverage for staff and patients. A passive DAS was designed by Boost Pro Systems to improve the corporate network within a key administrative office area, and due to poor external signal strength, a high-gain LPDA antenna was incorporated to maximise performance. The solution ultimately delivered 3G/4G/LTE voice and data, with multi-carrier support with carrier switching. The staff have reported improved productivity and operational advantages, while benefiting from enhanced health and safety.

Proving extremely positive for the large, complex environments of the NHS, DAS delivers an effective solution to indoor connectivity challenges that can extend beyond hospitals to other large enterprises.



A distributed future?

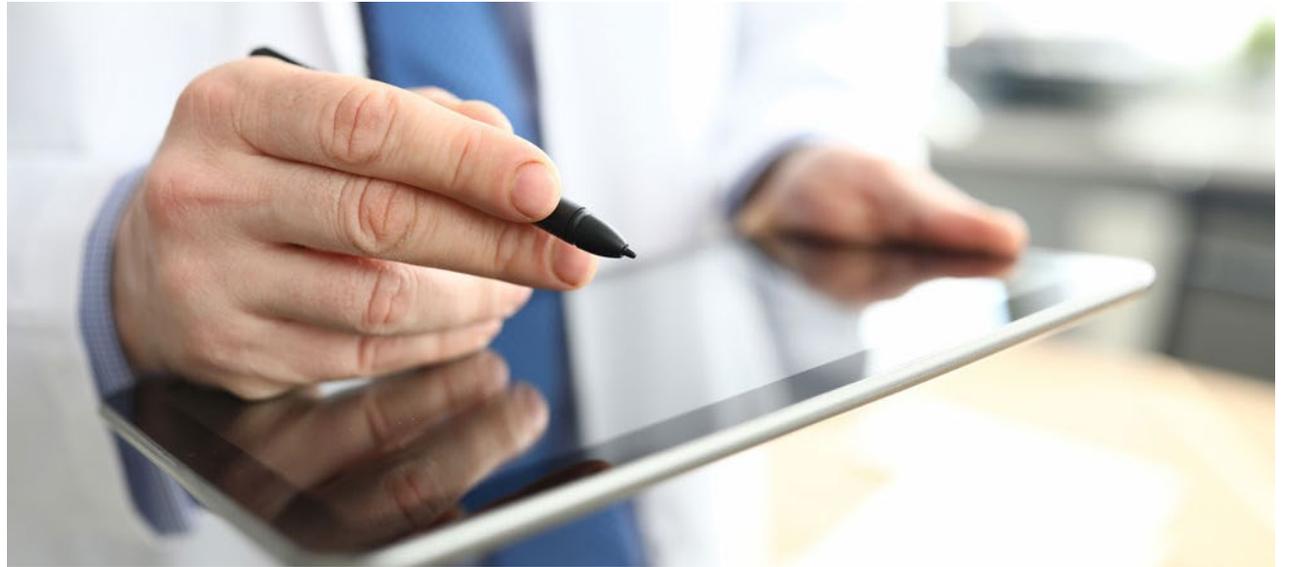
The DAS segment can expect to see strong growth throughout the enterprise world. Indeed, the DAS market was valued at US\$10.8 billion in 2021 by Future Market Insights and is expected to grow year on year by 11.1% to US\$12 billion by 2022, and achieve a compound annual growth rate of 9.5% over the next ten years to reach US\$29.7 billion by 2032.

However, is DAS truly the future of indoor connectivity for enterprise users? Opinions are divided.

“Many companies might be thinking about purchasing a DAS, leaky cable system or other similar approach to address coverage-related issues while trying to minimise active components like access points,” said Nispel. “However, a DAS is costly to deploy and can often lead to hidden node problems, where individual nodes can communicate with a wireless access point but not directly with other nodes. This issue is particularly common if only a single access point is connected to the DAS, severely limiting its capacity. Techniques like leaky cables can address only niche use cases, usually producing poor results.”

Some industry principles espouse WiFi as the answer for indoor connectivity challenges, particularly with WiFi 6E and WiFi 7 changing the marketplace.

“As for DAS providing cellular indoor coverage - the truth of the matter is that in the age of WiFi 6E and with WiFi 7 just around the corner, deploying a DAS is not going to give comparable results: neither performance and experience nor cost (both deployment and operational) will fit the needs of today’s networks in



terms of device density and experience expectations. For robust reliability, simplicity and cost efficiency, WiFi is the optimal indoor connectivity solution,” continued Nispel. “This is especially true in offices and institutions such as universities and hospitals, where in addition to the usual applications for real time communication, IP-based communication applications like Zoom and Teams are heavily used and almost entirely remove the need for ‘native’ voice connectivity. The high efficiency and high-capacity nature of solutions such as WiFi 6E will help organisations to create bespoke indoor networks which address the needs of enterprise applications and use cases today and tomorrow.”

However, other vendors believe

that WiFi is limited in its reach and effectiveness for enterprise applications.

“There is a perception that WiFi is an alternative for cellular communication, whether it is used for data offloading or WiFi calling,” said Kowal. “The reality is that there are limitations to what WiFi can do to meet cellular capabilities. WiFi still struggles with interference in large networks, roaming, variations in throughput with mobility, and security. Cellular is inherently built around each of these WiFi limitations. Also, from an end user perspective, many people do not feel comfortable attaching their devices to unknown WiFi networks. Cellular is more trusted and capable of handling mobility, prompting businesses around the world to invest in DAS solutions.”

As is so often the case, talks of a middle ground, with DAS an ideal solution for some enterprises but not others, seems most likely.

“Dedicated DAS deployments with base stations on site will still be the go-to model for large sites, but centralised base station deployments are needed to drive down the cost for enterprises and open up DAS to a wider market. Customers simply don’t have the money nor the space a dedicated DAS requires,” said Hourihane. “Virtualised RAN will help in a couple of years to drive the DAS with a cheaper radio source. Traditional DAS combined with a private 4G/5G service could also be suitable in the future and help businesses to deliver new use cases over the same infrastructure.” ■

No PoE, No Problem

Don't delay a project!

Find DrayTek APs that ship with an external power supply.



Find Your Solution

DrayTek

web: www.draytek.co.uk | tel: 0345 5570007



Getty Images / Red Bull Content Pool

Data driven wins

The Formula One™ season lasts eight or nine months, however, design teams are hard at work year-round to improve performance. Designing racing cars is a continuous process of integrating technology-driven innovations, making Formula One™ more than just a race; it is also a competition of technology. Behind the scenes, thousands of data points and dozens of applications come together to enhance race day results. Here, we explore how two racing teams upgraded their data storage and analysis in the search for gold

Oracle Red Bull Racing appoints HPE in race to the future

Oracle Red Bull Racing has sped its way to many victories across the world, with recent wins including the 2021 and 2022 Formula One™ World Driver's Champion: Max Verstappen, as well as the CONSTRUCTORS' WORLD CHAMPIONSHIP 2022.

The entire team is keen to push the car to the limit at each race. Insight-driven decisions, led by engineers, powered by IT and fuelled by data, can be the difference between winning and losing.

"We're a data-driven business and that data is our lifeblood in terms of how we develop and optimise these cars," said Oracle Red Bull Racing CEO and Team Principal, Christian Horner. "You only see our shop window at each Grand Prix, but you don't see what goes on behind the scenes with the technology that we're using and the boundaries that we're pushing."

In between races, the car is redesigned and rebuilt with customised specifications ready for the next track. Throughout a single season, a car can undergo 30,000 changes, involving 1,000 design elements per week. Every change in the process needs to be simulated, manufactured, and tested.

"For me, the perfect lap doesn't exist. When we start looking into the data, there are always things you can improve," said Verstappen.

Regulation changes

For the 2022 Formula One™ season, engineers were tasked to create under a new set of design regulations while staying within established cost caps. This made efficiency more important than ever.

"New regulations mean that whilst the team continues to innovate and push boundaries, we need to be very smart when it comes to the efficient use of resources, including how we get the most out of the IT estate that underpins car design and development processes," said Matt Cadieux, Oracle Red Bull Racing CIO.

Further changes in Formula One™ rules include limiting how many aerodynamics testing hours each team can run per week, using a sliding scale based on last season's performance. Red Bull Racing will have less time in the wind tunnel and computational fluid dynamics (CFD) simulation software than most teams due to its leading performances in previous years.

A software-designed platform

To meet these new regulations, Oracle Red Bull Racing partnered with Hewlett Packard Enterprise (HPE), which delivered a software-defined, composable platform based on HPE SimpliVity and HPE Synergy.

"Hewlett Packard Enterprise has partnered with Red Bull Racing for seven years, delivering cutting technology

solutions to both the factory in Milton Keynes and to every racetrack around the globe with our trackside solutions," said Adrian Lovell, CTO - financial services industry, HPE. "At the heart of this partnership is the data. In racing, where teams deal with extremely complex and constantly changing variables, including regulations, environmental conditions, and the tracks themselves, data can make the difference between winning or losing."

Today, some 80% of day-to-day business applications are running on HPE SimpliVity.

"The car changes every race, our software changes every race, and as a result our infrastructure has to change every race," said Chris Middleton, Head of IT Infrastructure Operations at Oracle Red Bull Racing. "We can bring new apps into play. We can bring new VMs, storage, networking. All of that can be added or removed, saving massive amounts of time."

To support the complex CFD process, which underpins the aerodynamic development of the car throughout the season, virtualised Citrix Workspace runs on HPE SimpliVity. Data cross-analysis can thus be completed on a single workstation, enabling engineers to produce more design iterations, faster. HPE Synergy combined with HPE OneView allows the quick reallocation of compute or storage resources as required, enabling the team to meet changing needs and maximise IT usage. The platforms' high density also

enables cost savings via reduced power, cooling and footprint expenses. Moreover, HPE Primera is utilised for tier one storage, and helps guarantee 100% availability.

The first step in optimising aerodynamics is CFD simulations, testing how different design elements enhance speed. This involves compute-intensive workloads such as physics simulations and 3D imaging.

"CFD models underpin the speed of design development at Red Bull Racing. CFD produces complex 3D, graphically intense models and therefore the team needs significant and efficient compute power to derive the best outcomes," said Cadieux. "These workloads run on HPE Apollo 2000, a high-performance computing cluster that provides the scale, speed, and efficiency the team requires to maximize CFD in a cost-effective manner."

Data from CFD simulations is confirmed at the team's wind tunnel in Bedford, where HPE Synergy provides compute for mixed workloads. 60% scale models are built and tested to choose the best design before manufacturing. Every second is optimised to gain valuable data, captured by a high-speed imaging system. These images, and all the data produced at the wind tunnel facility, are stored on HPE Nimble Storage, which delivers sub 0.5 milliseconds I/O latency for read and write operations.

Meanwhile, the use of HPE InfoSight, which delivers AI-enabled predictive analytics, enables the IT team to spend

less time managing disk resources, and allows to deep dive into storage metrics. This delivers a greater understanding of workloads and the most efficient use of resources.

“Naturally, the requirements for IT systems in racing, and especially at the trackside are high: They need to operate at peak performance levels and with very high availability, while being lighter and more compact than traditional solutions, and robust at the same time. Moreover, they need to be capable of coping with the power cuts that are frequent at racetracks, to ensure continuous data processing,” said Lovell. “With HPE SimpliVity at the core of Red Bull Racing trackside data centre, which resides in the hospitable environment of the garage at each race, the team is able to capture and analyse race data in real time. In a race, where every second counts, this data is critical to instantly optimize car set-up and support key decisions.”

Data meets real world

“That race weekend, when we hit the circuit, that is our first chance to see at full scale how those components are going to perform. Is it going to be reflective of what we saw in our theory? That’s where the data comes face-to-face with the real world,” said Zoe Chilton, head of strategic partnerships.

HPE SimpliVity acts as the core of the team’s mobile data centre, providing post-processing of race telemetry data,

as well as real-time insight to optimise car setup and support in-race decision-making. Its compact, robust, and seamless set up attributes make it ideal for trackside deployment.

“The data, thanks to the collaboration with our joint partner Citrix, can be accessed by engineers around the world through VDI environments provided by HPE,” said Lovell. “This setup allows the engineering team to directly analyse live data wherever that data resides with no delay. While the environment of a Formula One™ track is unique, many of the challenges faced are familiar to a large number of businesses. Real time simulation and data analysis are core to the success of more and more organizations. For both, HPE and Red Bull Racing, the insights won throughout these past seven years have been central to our work and the lessons HPE learns with every new race we then apply to the services and solutions we deliver off the racetrack.”

“Bringing HPE SimpliVity to support our trackside operations enables our trackside engineers to focus on car performance, knowing that they can rely on the IT infrastructure to deliver and back up the data that they need,” said Simon Kessler-Lyne, head of Event IT at Red Bull Racing.

The amount of time taken to transfer hundreds of Gbs of data from the car in real time on race days for post-process analysis has reduced by 78%, from nine to two minutes.

“It’s a massive increase in performance,”



said Cadieux. “What that means is we can get better answers quicker when we’re on the racetrack where seconds count.”

Back at the factory, data gathered at the track is received by the vehicle dynamics group. The datasets run on HPE Apollo 6500 to gain from faster interconnects for full utilisation of GPU resources for faster, better decision-making.

“Sensors capture hundreds of data points across the car, every time it’s turning a wheel on track, or even when we fire the engine up in the garage. We’re always learning,” said Chilton. “Our engineers pull apart the data from that race in so much detail to help understand what we need to carry forward to the next race.”

HPE’s solution has enabled rapid decision-making during race season with high-performance and cost-effective IT infrastructure, the agility to adapt to changes on and off track, and has accelerated race data post-processing by 78% compared with legacy infrastructure.

“Working with Hewlett Packard Enterprise is a hugely beneficial partnership for us. We’re able to be at the cutting edge of technology in a highly technical, highly stressed, environment,” said Horner. “There is no bigger challenge than Formula One™. It’s that marriage between creativity and data that has allowed us to achieve the success that we have over recent years.” ■

Mercedes-AMG Petronas selects Pure Storage for the win

One of the most successful teams in Formula One™ history is the Mercedes-AMG Petronas Formula One™ Team, which holds the record for the most consecutive constructors’ championship titles and for the most consecutive wins in a season.

Behind the scenes

Behind the scenes, an IT engine collects, stores and analyses many terabytes of data generated by the car, and more than 1 billion data points, in addition to other business interests, including lean manufacturing and social media. In order to accelerate decision making, the Mercedes-AMG Petronas team opted to undertake a modernisation programme.

In an industry where speed is everything, the IT team outlined gaining faster access to its data as the ultimate differentiator.

“For us, it’s about investing to develop a new capability, something that we can’t do

today but that we could tomorrow,” said Mercedes-AMG Petronas Formula One™ Team IT director Michael Taylor. “And if there’s a technology that makes this possible, the business case is much easier to justify.”

There were several challenges to be addressed in the search for a new solution. The piecemeal addition of new services, applications and simulators fuelled an exponential growth in data volumes, generating significant operational overhead in the organisation’s data centre. Moreover, managing different systems and infrastructure from multiple vendors was extremely complex, not to mention expensive. The setup also meant that applications resided in disparate systems, yielding inconsistent results across the business.

“We knew we needed to provide data services to the organisation at a cost point that is effective, but we also needed basic controls to secure the data and provide a certain level of performance,” said Taylor.

A fast-track solution

The Mercedes-AMG Petronas Formula One™ Team selected Pure Storage. The team standardised on Pure Storage FlashArray and FlashBlade, migrating more than 3PB of data, and utilised ActiveCluster for data safeguarding, which provides uninterrupted insights both on and off track, delivering a competitive advantage for Mercedes.

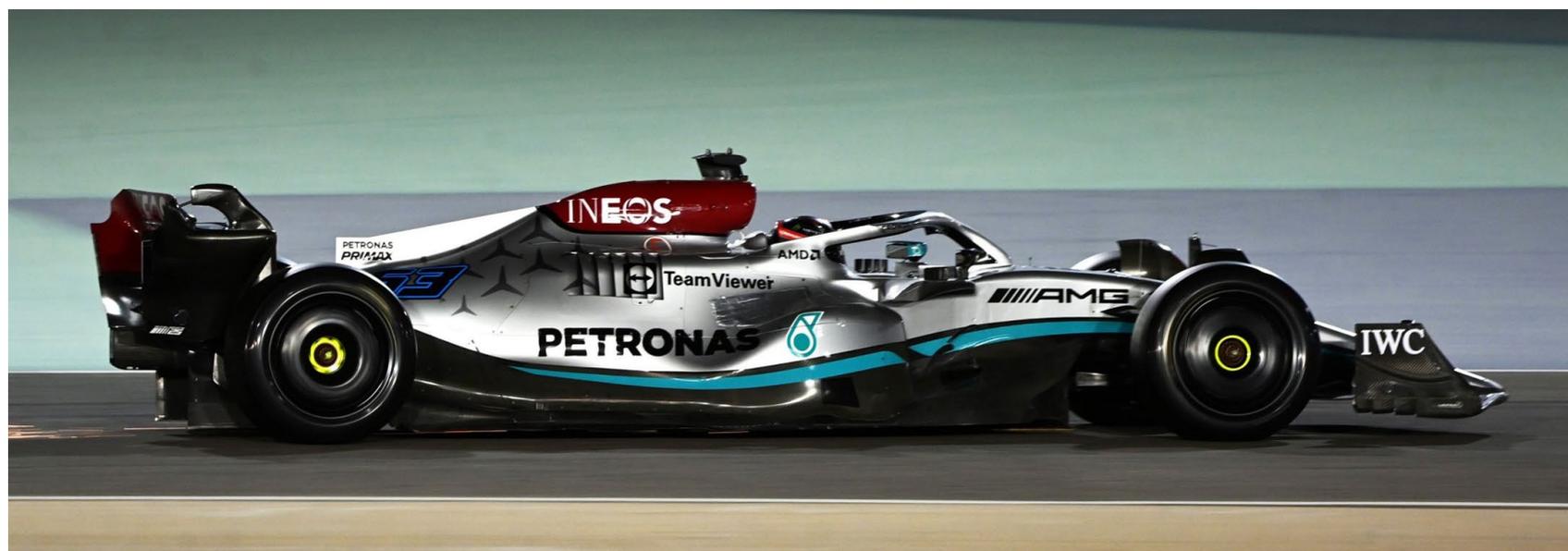
“The performance of Pure Storage was an immediate standout for us, but the simplicity of the offer made them absolutely different from the competition,” said Taylor. “They were taking the F1 approach to storage.”

Since moving to the modernised system, the team has experienced a 90% improvement in query times for database applications and 66% faster access to track-side files. Just one storage administrator is required to manage the entire environment, even with the

exponentially growing data volumes. Mercedes-AMG Petronas Formula One™ currently generates thousands of channels of data, augmenting and supplementing them with virtual channels. Going forwards, smart sensors will do some of the processing automatically, filtering out noise from insightful data, potentially during a race.

“We want to be knowledge-driven, so we must reduce operational friction and seamlessly use data as an enabler to make effective decisions,” said Taylor. “Pure’s architecture makes it very easy to provision storage and provide storage-based services in the data centre with the least amount of input but the most amount of control.”

Pure Storage’s solution has delivered fast-tracked decision-making for improved performance, built agility and resiliency into operations both on and off track, and reduced operational friction to support a knowledge-driven business environment. ■





Is 5G the answer network managers have been waiting for?

Tim Mercer, CEO, Vapour

The race for 5G connectivity in business is on. Telecommunications has finally evolved to keep up with the ever-increasing volume of traffic that moves around a corporate network every single day.

We've already started to see its potential, in smart cities across the UK and for mission-critical services demonstrating what it can really do. Therefore, organisations are understandably keen to embark on their own 5G journeys too.

After all, it could transform an enterprise by offering next-level speed and ultra-low latency, resulting in improved efficiencies, reduced costs, and better decisions. These are all reasons that so many IT teams are focused on 5G adoption, according to a recent Deloitte report.

But it would be wise not to get carried away. 5G sims still need to be treated with the same care and attention as any other component of the corporate network infrastructure. Otherwise, the security posture of a company's entire estate is at risk.

Although it seems we're nearly there, there's still work to be done at the source. To carry all the 5G traffic, major back-end network upgrades are required. Some carriers have been able to complete these, whilst others haven't.

To accelerate the roll-out, Ofcom recently announced a proposal enabling Vodafone and O2 to use the existing 4G infrastructure for 5G frequencies. Ofcom is answering the evidential demand for 5G services, but for those who paid more for their 5G spectrum, it looks like they've drawn the short straw.

Could this be a silver lining for customers? Perhaps Vodafone and O2 will be more inclined to offer more competitive rates for 5G services than some of the higher paying carriers. We'll have to see how this plays out. Either way, it shows that agility and adaptability around the 5G spectrum are a must for maximising the true advantages.

Whilst connectivity has been high on the IT agenda of every business since the explosion of remote working, arguably the biggest priority for network managers has – or should have – been security.

Hybrid working has created significant challenges for teams responsible for securing an organisation's estate across multiple locations, especially if the security focus has been at a network's edge, as opposed to it being in-built, by design, at the network's core.

However, any technological or organisational step change is likely to heighten security risks – it's par for the course with innovation and accelerated tech adoption. A strategic approach is therefore required to mitigate such risks, rather than operating on the fly.

That's why, as the 5G roll-out continues, network leaders must realise the security concerns that this technology brings.

Organisations are rightfully hungry for 5G connectivity – especially in rural locations and/or on temporary sites such as those in the construction industry, where flexibility and speed to deployment is critical.

But while 5G sims present an attractive connectivity option – whether as a primary or back-up service – companies would be foolish to throw all their data over a public 5G network, both for security and traffic visibility reasons. The technology needs to be run in the right way, if it is to function as a resilient business solution.

5G might be used as a failover, for instance, if a leased line service was to go down. But you can't just plug a 5G sim in and expect it to work. What happens to traffic visibility? And who will manage, control, and monitor the technology, if it sits outside of the corporate estate?

5G connectivity in the corporate world must be rolled out as a considered part of a private network strategy, especially if it will be relied upon by mission-critical applications. In fact, a recent survey showed that investment in 5G private networks will exceed tens of billions of dollars, validating that this is the future of corporate networks.

Routing multiple 5G sims via VPN into a network is one option, but this isn't ideal as the service isn't managed. Think about what happens if leased line connectivity goes off – a business wouldn't go straight to the carrier as they'd get no help. It would be no different with 5G.

Companies should therefore look to partner with private network specialists who can directly interconnect with the 5G provider, offer flexible usage with multiple carrier relationships, and provide complete transparency into network traffic, by bringing the mobile network into an SD-WAN infrastructure.

This approach will also allow for the sim to have a static IP address which enables the network manager to monitor data usage, application management, and threat analysis with a proactive application monitoring solution. This is how 5G can deliver the robust and resilient business solution demanded by all.

Although the 'plug and play' functionality

of 5G sims might be too attractive to let go, we must cast our minds back to the introduction of domestic broadband routers. This residential product seemed like the answer to the corporate world's prayers for improved connectivity. However, it just couldn't deal with the amount of data traffic on such a complex network. So, lessons need to be learned here.

Before organisations undergo this business-critical transformation, there is work to be done. But the future of 5G is promising. With a private network strategy in place businesses can achieve the speed, agility, and security that they are truly looking for. ■

MobileMark

antenna solutions

STAY
CONNECTED

with Advanced 5G
Antenna Solutions for
Autonomous Vehicles,
Public Transportation,
Precision Agriculture,
Medical IoT, Robotics,
and More!

www.MobileMark.com

Contact Us Now:

+44 1543 459555

enquiries@MobileMarkEurope.co.uk

Rolling out IoT to address county council challenges



Nick Sacke, head of IoT solutions, Comms365

As the country recovers from COVID-19, 2022 will be a year of recovery, and local authorities have a crucial role to play. Pressures continue to increase from the government to meet climate change targets, improve health and social care and ensure that local infrastructure continues to meet increasing demand.

Sustainability and climate change

Across the UK, we produce masses of waste. With non-efficient processes in place for collecting waste from public places and homes, councils and third-party contractors face a massive challenge.

IoT technology can dramatically improve current ineffective processes - from creating an optimally efficient route to collect waste to reduce carbon emissions, to emptying the right bins, at the right time, to improve green objectives. Sensor technology can not only indicate how full a bin is, but can also detect temperature and motion, to see if somebody has thrown something flammable in the container, as well as the bin tipping over or being misplaced. This information can be used to build a data profile which will provide a more efficient collections schedule and identify hotspot areas with potential problems.

Technology is becoming more efficient at determining different types of waste, particularly within underground storage, which can be useful for recycling efforts. IoT sensors can check how much glass is in a specific container by comparing the sonic 'signature' via intelligent algorithms.

IoT can additionally help councils and third-party contractors plan by knowing how much waste they will be collecting by real-time monitoring of waste in the bin lorry itself, which can help forecast cost and/or revenue. This could revolutionise payment models for contractors that are paid by weight.

With heavy regulations coming into play around air quality, and as society strives towards a greener future, local authorities must be more proactive. By tracking environmental elements such as pollution levels, CO2 concentrations and chemical pollutants in offices and classrooms, environmental monitoring will become a big part of both our indoor and outdoor future.

Integrating healthcare services

The IoT healthcare market is expected to reach US\$188.2 billion by 2025, driven by the pandemic and increasing focus on patient services. Technology can transform industries, reduce the burden on primary, acute and community care, as well as local councils. This was highlighted during the peak of the pandemic, with NHS hospitals implementing virtual clinics and remote monitoring to care for patients at home, while focusing on the ever-increasing COVID-19 cases. IoT technology enabled the collection of valuable real-time data to provide care to patients both in and out of hospital, while keeping them connected to healthcare professionals. The data helps to automate the mapping of activities into a profile around an individual, which can be analysed and shared with the care organisation and local authority.

Patient health and vital signs can be recorded from home, such as heart rate, blood pressure and temperature, meaning clinicians' time can be used elsewhere, enhancing the efficiency of existing processes. Specialists can be alerted when deterioration or health concerns are detected to enable immediate intervention and targeted care delivery. By flagging issues earlier and preventing the escalation of problems while the individual is at home, the need for them to go to the hospital for check-ups or treatment is mitigated.

Technology can also be used to reduce variations in care by identifying patients who may be at risk and have not seen their GP, or those in rural and remote areas, by providing access to interact with and monitor people in places that have been traditionally harder to reach. IoT technology has greatly improved accessibility and productivity in remote healthcare, providing a mechanism to help the NHS extend care beyond the hospital.

Local infrastructure

With almost 50 shops closing each day on the high street during the first six months of 2021, and UK shopper footfall dropping, local authorities are looking for alternative initiatives to encourage people back to the high street. If shoppers are looking to travel to physical stores once more, the parking experience should be painless - or else they'll return to online shopping.

It's estimated that motorists spend two months of their lifetime searching for a parking space. What if this could be cut down with the use of technology? What if an individual's mobile device was to alert them in real-time where a parking space was? Better yet, what if this space could be reserved, or set up a subscription model to park monthly? It's all about data collection and a better, more informed use of this data. By incorporating electric charging and disabled bays, re-engineered and revitalised parking solutions will boost council revenue and provide more efficient and customer-pleasing services, regenerating the shopping experience.

The rising cost of living, energy and fuel poverty

At the time of writing, inflation had just breached 5.5% and is on course to exceed 7%. Oil and gas prices are rising, producing knock-on effects in raw materials and transportation costs, energy, shopping basket prices, etc. The current economic climate is creating a punishing set of circumstances, especially for the elderly and those on low incomes.

There have already been several cases reported of the vulnerable making choices between heating or eating, which is of grave concern. Many of these vulnerable citizens live in local authority housing, so what can IoT technology do to assist?

In the case of fuel poverty, monitoring temperature and environmental conditions in vulnerable households, together with energy consumption from the boiler will create a profile of energy use, highlighting which of the population require targeted interventions to assist with fuel bills and other assistance. Smart radiators can be implemented to heat sections of the home that require it at different times of day, providing energy savings and improved living conditions. IoT data could also profile and identify potential dwellings that have insulation, leaks, and other structural issues that affect the housing integrity and prioritise intervention.

Conclusion

IoT technology is advancing to meet increasingly imposing challenges. We're not only seeing an uptake in interest and the use of these solutions, but the technology itself is becoming increasingly cost-effective, adaptable, and easier to deploy and maintain. COVID-19 has prompted a greater need for local councils to be forward-thinking in how technology and data can help towns recover now and strive in the future. The value of IoT technology and the real-time data it collects is being recognised, and will help to inform better decision-making, introduce early interventions and reduce the cost of changing practices.

But for this to work in practice, there is a significant need for a cultural shift in the relationship local governments have with technology. The technological solutions must be designed around the user, creating a better experience, while ensuring any potential barriers are removed. The guiding principle for deploying technology as an enabler of these more streamlined processes is simplicity and invisibility to the user, while collecting valuable data for insight. ■

CP Critical POWER
Supplies ■ Projects ■ Support

ONE SUPPLIER...

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

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

- Electrical installation & consulting services
- New thermal imaging capabilities
- Power ■ Cooling ■ IT infrastructure

- 3-Year warranty
- World class impartial advice saving you time & money
- Call now for a FREE site survey & health check
- Nationwide sales & engineering team, on hand 24/7



Design & Build



Cooling



Batteries & Accessories



Generators



Onsite 24/7 Services



UPS



Data Centres



Voltage Optimisation



PDU



Racks & Enclosures

**Critical POWER :
When it matters most**
criticalpowersupplies.co.uk



Choosing the right wireless solution for your business

Patrick Hirscher, wireless market development manager, Zyxel Networks

Wireless technology is now an integral part of day-to-day life for individuals and businesses alike. Just as with electricity, we rarely stop to think about the importance of wireless technology until there's an issue with our network. Now more than ever before, it is imperative that organisations tailor their wireless solutions to meet the specific needs and demands of the business.

The shift in consumer networking needs

The shift towards remote working, combined with the surge in energy costs, has seen employees flocking to work from cafes, restaurants and pubs in an effort to reduce their heating bills at home this winter. But this influx of laptop workers has meant that for many small businesses, their wireless networking solutions no longer meet the demands of their patrons.

A strong wireless connection is not only imperative to retain and attract this newfound customer base. Small businesses are now dependent on wireless technology for their daily

operations. From their cash terminals to their order points, the majority of hospitality venues have incremental equipment that is reliant on a stable wireless network.

Previously, WiFi routers with embedded Access Points were enough to meet the needs of small businesses. However, the increased dependency on wireless connectivity from both customers and businesses alike has meant that small businesses now need to invest in an external Access Point, to support the increase in the number of users looking to connect to the network.

Investing just a small amount of money on a basic Access Point will not only improve the day-to-day operations of a business, but also help attract the growing number of remote workers, improving the bottom line for businesses at a time when it is under pressure.

Density vs distance

Larger scale businesses operating across multiple rooms and floors, such as offices or hotels, will likely already have Access Points integrated into their networking infrastructure.

However, where many of these mid-sized companies run into connectivity troubles results from lacking the tailored solutions their business needs.

For example, in a scenario where there is a high density of people in a small area, like in a conference room, classroom or the London Underground, powerful Access Points are required. Investing in multiple, cheaper Access Points will not be an effective solution, as these APs will not be able to handle the quantity of users and devices attempting to join the network at once. In an instance like this, businesses must invest in two or three powerful Access Points, depending on the quantity of users and devices.

Comparatively, in a hotel where rooms are spread across a long corridor, the density of users is lower, but the distance from the router will be far greater, meaning that guest users located further away from the router will struggle to connect. In this instance, one or two powerful Access Points will not solve this problem. Rather, businesses should invest in multiple, lower power Access Points to spread along the corridor. This will enable guests, regardless of their location, to connect to the router seamlessly.

Securing the network

In recent years, businesses across the globe have become the target of large-scale cyber-attacks by malicious actors. According to the UK Government's Cyber Security Breach Survey, phishing attacks accounted for 83% of all business cyber hacks in 2022. For organisations that have access to sensitive data, falling victim to such an attack could have catastrophic implications for the company.

To prevent sensitive data from getting into the wrong hands, businesses should consider investing in an Access Point that has a security component. Fairly new to the market, these APs can be centrally managed via a cloud platform and can filter out any unsafe web content and prevent users from accessing the data streams of others, preventing malicious actors from spying or stealing the information of others.

While these security profile embedded APs have a premium price point, they eliminate the need for a separate security gateway device, saving businesses money in the short and long term.

PRODUCTS

The **Aruba 650 Series** Indoor Access Point takes advantage of the new capacity of the unlicensed 6GHz band. With 7.8Gbps maximum aggregate throughput, the 650 Series meets the requirements for WiFi 6E certification with room to grow. By leveraging the 6GHz band, the AP delivers peak performance and far greater capacity than previous generations of WiFi. With up to 1200MHz of new channels, capacity is nearly tripled to meet growing demand due to bandwidth-hungry video, increasing numbers of client and



IoT devices, and growth in cloud. The 650 Series AP includes Aruba's patent-pending ultra tri-band filtering, which enables enterprises to take advantage of the high end of 5GHz with the lower end of 6GHz without experiencing interference. This is important because there is only 95MHz between 5GHz and the 6GHz, which would cause interference between the two bands. The ultra tri-band filtering is fine grained and dynamic to allow enterprises to make full use of available spectrum without creating coverage gaps or islands.

The **Cisco WiFi 6E-compliant Catalyst 9136 Series** takes advantage of the 6GHz band expansion to produce a network that is more reliable and secure, with higher throughput, more capacity, and less device interference. The access points come with two 4x4 radios and one 8x8 radio and provide a host of features.

WiFi 6E technology extends WiFi 6 into the 6GHz spectrum, bringing faster speeds and lower latency while also providing more security to the network. Dual Multigigabit Ethernet provides power-redundant uplink ports, each with speeds up to 5Gbps. All speeds are supported on Category 5e cabling, as well as 10GBASE-T (IEEE 802.3bz) cabling.

Redundant powering provides hitless performance during failover.

Smart AP causes the access point to change its power consumption to reflect its current client load. An access point will typically operate on the radios provided to it irrespective of how many clients are connected.



The **Ruckus ZoneFlex R850** access point is based on WiFi 6, bridging the performance gap from gigabit WiFi to multi-gigabit WiFi in support of the insatiable demand for better and faster connectivity.

The R850 makes it easy to deliver reliable, secure, ultra-high-performance connectivity to large enterprises, public venues, convention centres, and other challenging environments.

The high capacity dual-band, dual-concurrent WiFi 6 (802.11ax) access point supports 12 spatial streams (8x8:8 in 5GHz, 4x4:4 in 2.4GHz). The R850, with OFDMA and MU-MIMO capabilities, efficiently manages up to 1,024 client connections with increased capacity, improved coverage and performance in ultra-high dense environments.



Juniper Networks' **AP45** is a tri-band device with a dedicated fourth radio and a dynamic, 16-element vBLE antenna array. It enables accurate and scalable location services, including user engagement, asset visibility and contact tracing with no battery powered BLE beacons or manual calibration required.

The AP45 access point series is a four-radio, four-spatial stream 802.11ax access point with maximum data rates of 4800Mbps in the 6GHz band, 2400Mbps in the 5GHz band, and 1148Mbps in the 2.4GHz band. The dedicated fourth radio functions as a network, location, and



security sensor, as well as a synthetic test client radio and a spectrum monitor.

Juniper's AI platform automates and optimizes the new features in 802.11ax (WiFi 6). Its AI for AX capabilities optimizes basic service set (BSS) colouring, improves AP-to-client data transmission scheduling (OFDMA), and assigns clients to the best radio to boost overall network performance.

Incorporating the 802.11ax-standard target wake time (TWT) capability and Bluetooth 5.1 into the AP design extends the battery life of new and existing IoT devices as they connect to the network.

DrayTek's VigorAP 802 is a portable wireless mesh access point, compact and easy to use either wirelessly or wired, enabling full use of the broadband potential.

The VigorAP 802 comprises an 802.11ac dual-band wall-socket WAP with a built-in power adaptor. It features advanced AP-assisted roaming, band steering and airtime fairness technologies, designed to boost signal and speed, ensure perfect coverage and create a smooth wireless connection. The VigorAP 802 can supply Wireless LAN connectivity as a mesh node, access point or wireless repeater

and can optionally be a LAN uplink, with its Gigabit LAN port - providing flexible, tailored connectivity for unique business needs.

The Plug-n-Play technology enables users to automatically configure a new VigorAP 802 wireless access point into the network. It can be managed centrally through the VigorConnect management system on a local network, or fully managed remotely across sites with VigorACS, DrayTek's central management platform. Both systems allow scalable provisioning, configuration, scheduled firmware updates and large-scale management.





Please meet...

Neil McLoughlin, UK Field Chief Technology Officer, Nerdio

What was your big career break?

I've worked in the End User Computing (EUC) sector as a consultant for over 15 years having started my career at Philips Semiconductors, before moving to Computacenter where I focused on rolling out Citrix VDI to 4,000 staff at the Nationwide Building Society. I've been involved with all sorts of different technologies over the years and have really drilled into the detail when it comes to the best way to meet the EUC needs of enterprises.

But it is joining Nerdio which I consider having been most significant from a career perspective. It's my first role working for a vendor. Nerdio has propelled me to another level and really expanded my non-technical skillset – things that I would never have been exposed to in my previous jobs. Working at a startup opens your eyes to a different world and you get involved in everything: sales, marketing, business development, along with helping channel partners to architect solutions for clients. The pace, the conversations, the skills required are on a different level to anywhere else I've worked and I am loving every minute of it.

Who was your hero when you were growing up?

I'll give a slightly cliché answer in that it is my father. But the 'why' he is my hero is not necessarily a common one. My dad was paralyzed down one side of his body his entire life and, three months ago, diagnosed with Motor Neuron Disease – that's the same illness that Dr Stephen Hawking had. He's had a difficult life, but through his immense strength and drive, he became a serial entrepreneur and set up various successful businesses. Physically the odds have been against him, but he has had so much grit, determination and unwavering focus to live life to the max. I think everyone can draw inspiration from that.

I'm disabled myself. I was born three months premature, and my left leg was amputated after I contracted gangrene. Seeing my dad overcome his challenges showed me how to harness the strength and desire to carry on with life as normal no matter what obstacles are put in your way. So, I sky dive, climb mountains and lead a very active life.

What would you do with £1m?

I would use it to help people who are less fortunate than myself. I think sometimes we need to stand back and realize just how lucky we are to enjoy life without focusing on the pressures of the day to day. Specifically, the NHS doesn't serve amputees that brilliantly with prosthetic limbs so I would help kids and young adults with the money to get them access to the best equipment available, which would make a real tangible difference to their lives.

Where would you live if money was no object?

I'd move abroad to a nice large villa in Portugal by the sea, mainly for the amazing seafood that I could gorge on each day! I live in Manchester so I am used to rain and cold weather. When I retire, I want to leave that behind and would love to live somewhere where the climate is nice and warm.

Which law would you most like to change?

I know it is hugely complicated, but I would like to introduce legislation which makes the right to die legal especially if you have a terminal illness. Seeing people suffer with an illness like Motor Neuron Disease is absolutely horrific and you should be able to choose if you don't want to continue anymore.

The Beatles or the Rolling Stones?

Beatles! Their music is iconic, although I missed out on experiencing 'Beatle-mania' myself as I wasn't born then.

If you could dine with any famous person, past or present, who would you choose?

Probably Elon Musk. I am fascinated by human performance and what makes people tick, especially when it comes to drive and motivation. I'd love to talk to him about this

to understand where his amazing ideas and work ethic comes from. I'd take him for a steak at a Hawksmoor restaurant.

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

I'm a massive consumer of motivation and self-helps books, but I guess to summarize everything I've read, it's to get what you want from life, you have to put the work in. Whether that's from a career, health, financial perspective or anything else, with hard work, focus and willpower comes success. The Compound Effect by Darren Hardy is super

example. He talks about how small, everyday changes can make a massive impact to your life over time – just like compound interest in finance.

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

I would say teaching. I don't know any other career where you could make such a huge impact on so many people's lives although teachers may tell you different story as it seems extremely hard work. I'd obviously teach computing. ■

BIG ON CHOICE

Choice is important that's why we have developed the markets most versatile range of rack solutions. From wall mount to open frames with a huge choice of cable management options, to racks designed for the deepest and heaviest servers and multicompartment racks designed specifically for co-location environments, we have a product to suit the most demanding of applications. When choice and options matter, you can be sure there is a solution within the Environ range from Excel Networking Solutions.

Visit Environ:
excel-networking.com/environ-racks

excel
without compromise.