JUNE 2023
networkingplus.co.uk

NETWORK+

Drilling for data

Data silos are a problem in established telco companies

David Shannon, SAS UK & Ireland, p5

Edge vs cloud? Don't believe it

They both need secure remote access

Alan Stewart-Brown, Opengear, p7

Questions and answers

Top Gun was one of the most influential films

Mark Yeeles, Schneider Electric, p16

MOVEit breach highlights risks from supply chain exposure

British Airways (BA), the BBC, Boots, and thousands of other major organisations have had personal data and bank details compromised following the exploitation of a zero-day flaw in file transfer system MOVEit.

Zellis provides HR and payroll services to clients in the UK and abroad, including the BBC, BA, Boots, and the NHS. Through Zellis' use of third-party software MOVEit, hundreds of UK businesses now face the horrifying prospect of having private data held to ransom.

Following the first reports of a zero-day vulnerability on 31 May, Zellis took swift remedial action in isolating the server hosting the MOVEit software, engaging an incident response team, and notifying those affected and the authorities.

Cybersixgill observed activity on underground sources related to the MOVEit flaw and interest in the data stolen in related attacks, reports Delilah Schwartz, security strategist, Cybersixgill.

"This activity includes posts on multiple Russian cybercrime forums seeking the data from Zellis-related victims of the MOVEit attacks. In the posts Cybersixgill collected from a forum member, they expressed an interest in a wide range of cybercriminal activity, including ransomware, carding, bots, SIM card swaps, stolen databases, remote access trojans (RATs), and information stealers," says Schwartz. "In one of the posts from a top dark web forum, a member specifically requested data from UK-based victims of MOVEit attacks, offering up to $100,000 for the requested content…"

The BBC has warned employees of stolen data including staff ID numbers, home addresses, NI numbers and dates of birth, while other companies have warned of bank details being compromised.

"This attack looks like a case of triple extortion, whereby the attacker targets both the company whose data they have as well as its customers warning them of data exposure until payment is made," outlines Alon Schwartz, cyber security researcher, Logpoint.

Russian cybercriminals behind the Clop ransomware have claimed responsibility for the attack and are now contacting the affected companies to negotiate ransoms.

"It's important to note the possibility of the use of stolen data in further social engineering attacks. BA, for example, noted payment information of its employees was stolen, but organisations should expect the bulk of data to be ransomed or uploaded to a leak site," says Timothy West, head of threat intelligence, WithSecure. "It's yet another reminder of the risks posed through supply chain exposure."

All software vendors battle security vulnerabilities, but vulnerabilities like this one can have severe consequences, which may be unfairly borne by the victims who use the software, explains Wicus Ross, senior security researcher at Orange Cyberdefense.

"Writing secure software can inflate costs for a vendor, which may disadvantage it in the market, so shortcuts are often taken," says Ross. "This is how 'security debt' is accrued and passed on down the software supply chain. Any time a vendor makes a deliberate security compromise, or honest security mistake, the victims of a resulting cybersecurity incident will have to absorb the costs."

Interestingly, Clop hackers now claim that they do not have data from the BBC, BA, or Boots.

"We don't have that data and we told Zellis about it. We just don't have it. We are an old group and have never deceived anyone, if we say that we do not have information, then we do not have it," said the hackers in an exchange with the BBC.

This raises an intriguing question: is Clop lying, or has another unknown hacking organisation stolen the data before or during the breach? ■

IN DEPTH: Network optimisation p9

Register for Networking+

British Army to benefit from smart bases with new BT MOD WiFi deal

BT has secured a major new networks contract with the Army – paving the way for the rollout of smart bases across the UK.

The company's business unit has won the five-year contract with the British Army to deliver a managed WiFi service, dubbed MOD WiFi. The deal will see BT provide managed secure WiFi across 162 new UK army sites, with the future potential to expand the contract to other Defence customers, including the RAF and Royal Navy.

The new contract will expand on the existing 200 Ministry of Defence (MoD) sites that BT's Defence team currently manage in the UK, Cyprus, and Germany, following over a decade of partnering with the MoD for its WiFi network requirements.

It will deliver a huge digital infrastructure boost, with a managed firewall built-in for enhanced security. Soldiers, who may currently struggle to receive connectivity in remote base locations, will now benefit from enhanced contact with loved ones and ability to relax during their down-time through access to digital platforms thanks to free, fast and reliable internet. The delivery programme covers all buildings in the sites being equipped, including offices, hangars, training facilities, technical accommodation, and workshops. All recreation spaces, messes, sports and dining facilities will also be covered by the service.

The connectivity will also provide the foundation for smart bases to begin rolling out over the next 12 months, enabling sites to improve the digital experience for military personnel, enhancing security with smart surveillance and intelligent Building Entry Systems, and supporting net zero ambitions by maximising building occupancy for more efficient energy consumption.

"This is another critical delivery under the ambitious British Army Digital Transformation Initiative – Programme THEIA," said Major General John Collyer, The British Army director information. "We are thrilled to partner with BT for the Army Estate Wide Internet work – which will deliver ubiquitous internet access across our estate – for business use, research, leisure, gaming, innovation, trials and more. Another leap forward, and I thank the staff of BT and in Army HQ for their Herculean work getting us to this stage. It will make a huge difference for our people and our outputs."

"The opportunities and threats posed by digital technology mean the Army needs the most reliable and secure networks possible – and we're proud to be a trusted partner that can deliver for them. This new managed WiFi service from BT will provide important connectivity across areas of training, business and welfare," said Ed Stainton, director of major government at BT. "Crucially, the contract will also lay the foundation for Front-Line Commands to introduce smarter ways of working, unlocking the benefits of new technologies on MOD Wi-Fi that will provide efficiencies, enhance productivity and increase security."

BT has already been working in partnership with the Army to establish a smart base in Larkhill, South West England, with a digital infrastructure that incorporates fibre broadband and private 5G. The base uses technology such as HD cameras and sensors, facial recognition, smart building entry and management, digital signage to relay tailored messages to different audiences, and secure printing. ■

Loughborough University DC redesigned from ground up

Schneider Electric has delivered a new data centre modernisation project for Loughborough University in collaboration with on365.

To overcome a series of data centre challenges including requirements for a complete redesign, modernisation of legacy cooling systems and improved cooling efficiencies, and greater visibility of its distributed IT assets, Loughborough worked with on365 and Schneider Electric to undertake a major modernisation project at its Haslegrave and Holywell Park data centres.

Delivered in two phases, the project saw on365 firstly modernise the Haslegrave facility by replacing an outdated raised floor and deploying an EcoStruxure Row Data Center solution. The deployment of this integrated row-based data centre solution has significantly improved the overall structure, enabling an efficient data centre design.

During the upgrade, on365 also brought other parts of the infrastructure under the IT department's control, using new InRow DX (direct expansion) units to deliver improved cooling reliability and provide it with greater ability to cope with unplanned weather events, including heat waves, which had adversely affected its IT and cooling operations in the past.

Use of the EcoStruxure Row Data Center solution also created new space for future IT expansions and extended a 'no single points of failure' design throughout the facility.

This made the environment more suitable for a new generation of compact and powerful servers, and the solution was replicated at Holywell Park thereafter. Further improvements in resilience and efficiency were also achieved by replacing legacy UPSs with Schneider Electric's Galaxy VS UPS with lithium-ion batteries, which offers up to 99% energy efficiency, without compromising availability.

"At the foundational level of everything which is data-driven at the university, the Haslegrave and Holywell data centres are the power behind a host of advancements in sports science, and our transition towards a more sustainable operation," said Mark Newall, IT specialist at the University of Loughborough. "Working with Schneider Electric and on365 has enabled our data centre to become more efficient, effective and resilient."

Alongside the new EcoStruxure Row Data Centre, the university upgraded the software used to manage and control its infrastructure.

Loughborough has now deployed the company's EcoStruxure IT platform, providing it with enhanced levels of visibility and data-driven insights that quickly help to identify and mitigate potential faults before they become critical.

This, in conjunction with a new three-year Schneider Electric services agreement delivered via on365, has given the university 24x7 access to expert maintenance support. The university also utilises a large distributed, edge network environment, which has in-excess of sixty APC Smart-UPS single-phase UPS's protecting it. As part of its services agreement, all critical power systems are monitored and maintained via EcoStruxure IT, providing real-time visibility and helping IT personnel to manage the campus network more efficiently. ■

UK-Singapore Cyber Dialogue to strengthen collaboration

Cyber chiefs from the UK and Singapore have come together to strengthen cyber collaborations with the new UK-Singapore Cyber Dialogue improving collaboration around the Internet of Things (IoT) security, app security and cyber skills development.

The countries have discussed the cyber threat landscape, deterrence strategies against, international cyber capacity building, international cyber policy issues including in the UN, and the role of public-private partnerships in cybersecurity.

The collaboration comes after The National Cyber Security Centre warned that Lockbit was the most deployed ransomware variants across the world in 2022, as organisations across a wide range of critical infrastructure sectors have faced serious disruptions.

"It is great to see governments coming together to unite against the ever-prevailing cyber threat, which all too often causes disruption across both public and private organisations around the world. We have seen many attacks in recent times that provide examples of cyber criminals only becoming more sophisticated in their approach, highlighting an even bigger need to come together as one," said Achi Lewis, area VP EMEA for Absolute Software. "Technology, such as self-healing technology, which can freeze and cut off vulnerable devices from a network and automatically update systems is one area that international collaboration can boost, and the sharing of technology and knowledge will help to build resilience for these tools. While prevention is important, ensuring that businesses and global governments are prepared to react when at attack occurs, not just if, is just as vital, and this is the kind of knowledge that global collaboration can lead."

"Recent attacks have underscored the crucial need for international collaboration. Governments, organisations, and individuals face unprecedented risks, necessitating a united front against malicious actors. By pooling our skills, technology, and knowledge, we can fortify our cyber defences. Learning from one another will better equip us to fight against future attacks, which are inevitable, building cyber protections that will reduce the wider spread disruption we are commonly seeing," said Suid Adeyanju, CEO of RiverSafe. ■

EDITORIAL:

Editor: Amy Saunders
amys@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Paul Dant, Mark Oakton, Alan Stewart-Brown, Alex Barter, Gareth Mitchell, Joshua Hughes, Mark Yeeles, Charlie Bellsham, Ciaran McCloskey, David Shannon

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

© 2023 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

Data teams are overextended

Matillion and Vanson Bourne have released findings of a survey in a new report, 'Data Productivity: A Survey of Data Experts.' The survey data offers insights from data team practitioners and leaders on how they manage the increasing complexity of unprecedented amounts of data, team workloads and overall performance at work.

Survey results illustrate that data teams are overextending themselves to meet business demands. 84% of respondents described the volume of their workload as exceeding their capacity, while 90% reported an increase in their workload over the last year, a challenge that will only grow if not addressed soon.

Additional key points from the survey include:

Teams spend too much time at work integrating, collecting, and transforming data rather than performing strategic work. For nearly 40% of respondents, this work takes between a day and a week to perform per project. 34% of respondents said this process takes 3-5 hours to complete per project — a sizable chunk of the typical 8-hour workday. Employees using slow, inflexible pipelines can't get the right information when they need it.

Data professionals spend too much time pulling from and unifying a high volume of data sources to build their data pipelines, which only delays the transformation process. 41% of respondents reported that their company uses 51-100 data sources, and 22% reported that their company uses 101-200 data sources. The sheer number of sources these experts use becomes a burden because they drastically increase their workload.

Employee burnout is on the rise, leading to challenges with talent retention for employees who enjoy their work. More than a third of respondents described feeling at least some burnout, with 19% feeling very burned out. 74% of employees responded that they feel very motivated at work.

Low-code and no-code tools are emerging as a primary strategy for companies to transform business-ready data. Sophisticated, visually guided low-code environments help create accurate, maintainable, and self-documenting code. These solutions make it possible for team members with less coding expertise to pull and transform necessary business data. Cost-effective and agile, these solutions also help end tribal knowledge, which can alleviate the challenges associated with employee turnover.

"This research highlights the data productivity pitfalls that modern data teams experience on a day-to-day basis," said Ed Thompson, CTO and co-founder of Matillion. "By taking note of these results — and partnering with organizations like ours to find solutions – businesses can empower their data teams to perform and prioritize impactful projects rather than the transformation of data; assure key decision makers with precision in their business decisions; and make it simple and cost-effective to deliver the right data to the right person at the right time. At a time where change is rapid, complexity is growing and the appetite for the right insights at the right time is voracious, addressing data productivity issues changes the game. If organisations don't take these challenges seriously, not only will they cost money and time in lost resources, but will expose the talent pipeline to employee burnout and turnover." ■

Email impersonations comprise 99% of threats

Malicious emails have reached a crescendo in 2023 according to the latest report from Fortra.

Email impersonation threats such as BEC currently make up nearly 99% of threats, and are proving to be the most difficult to block as social engineering helps cybercriminals successfully deceive both end users and the security tools designed to protect them.

Moreover, more than 60% of email threats impersonated a well-known brand name such as Microsoft or Google. 36% of email display names are altered to a more granular level and pose as specific individuals. Google is the most abused email platform (67.5% of recorded attacks in 2023), with Microsoft following close behind (18.3%). Additionally, BEC actors are moving toward intercepting payments; instead of asking for an explicit amount, attackers ask for an unspecified sum owed. Office 365 phishing attack volumes have doubled since the fourth quarter of 2022. Generative AI is trending among cybercriminals - ChatGPT, and other such language models, are giving criminals the tools to craft well-written messages at scale and avoid the poor spelling and grammar that frequently mark phishing attacks.

"It isn't hard to find someone who has fallen victim to email impersonation attacks. Social engineering combined with advancing technology such as generative AI has made attacks more advanced and harder to spot," said John Wilson, senior fellow, threat research at Fortra. "Organisations must rethink how to defend against such threats. For instance, consider if your security awareness training explores enough of current impersonation techniques, as well as how applying algorithms through machine learning can help to detect anomalies and patterns in order to accurately detect signatureless email threats at scale." ■

Register for Networking+

Building & Managing your IT at the Edge

As organisations deploy their IT at the edge, it is quickly becoming a critical part of their operation. Organisations are now starting to adopt AI and other technologies as complex IT environments start to move to the IT edge. With edge computing becoming indispensable, any unanticipated downtime has the ability to disrupt or completely paralyse an organisation altogether.

Vertiv's™ end-to-end solution portfolio of rack enclosures, critical power, rack PDUs, cooling, and out of band access are designed for rapid deployment and quick-and-easy-start-up, ensuring your mission-critical applications run uninterrupted.

Collaborate IT Limited, a long-standing **Vertiv™** platinum partner specialising in Vertiv's™ core brands **Avocent®**, **Liebert®** and **Geist™**, have over 20 years' experience working with data centres and server rooms. Collaborate IT's strategic relationship with Vertiv™ ensures quality and reliability to help you take your IT to the edge and beyond. With comprehensive services offered ranging from site surveys to preconfiguration and installation services, you are in safe hands with Collaborate IT and Vertiv™.

When building your IT at the edge, Collaborate IT can help select a combination of Vertiv™ solutions that suit your needs to help reduce complexities and simplify IT deployments at the edge. The Vertiv™ solution portfolio allows you to standardise globally, build on reliable power infrastructure, remotely view capacity and identify environmental threats. In addition, organisations can remotely manage heterogeneous environments securely from anywhere at any time.

IT Rack

Vertiv™ VR IT Racks: Reliable quality & industry standard flexible design with comprehensive range of rack accessories for maximum compatibility at the edge.

Backup Power & Protection

Vertiv™ Liebert® UPS: Provides reliable backup power & protection for servers, storage, telecoms & networking equipment at the edge.

Rack Power Distribution

Vertiv™ Geist™ Rack PDUs: Remotely monitor power, manage IT loads & power control troublesome IT devices at the edge.

Environmental Monitoring

Vertiv™ Geist™ WatchDog: Remotely identify environmental threats at the edge with proactive monitoring & alerts.

Out-of-Band Access

Vertiv™ Avocent® ACS Serial Console: Remotely deploy & manage your network infrastructure at the edge, even when the network is down.

Curious about building your IT at the edge?
sales@collaborate-it.com
https://www.collaborate-it.com

Productivity stunted by unreliable technology

Some 35% of employees are having their productivity stunted by insufficient, slow, and unreliable technology – yet 27% of CIOs say home distractions are the culprit. These are among the findings of new research by Apogee Corporation.

The research highlights the impact unreliable workplace technology is having on employee performance and collaboration. A further 21% of employees say that a lack of team connection and collaboration opportunities when working from home is hindering their productivity.

This contrast in perception is threatening to isolate employees from their organisation and colleagues. For 46% of employees, access to the right technology is key to feeling connected across hybrid work environments – yet 56% say technology is unreliable or completely non-existent when working from home. 28% employees also say they are unable to do their job properly as a direct consequence of poor digital collaboration with technology. As a result, 79% of employees don't feel optimistic about the future of work – with 46% saying that a lack of access to the right technology is fuelling this negativity. Most CIOs share this outlook, with just 5% claiming they are optimistic about the future of work.

The research also revealed a strong disconnect between CIOs' and employees' workplace ideals. A quarter of CIOs believe that training and career development is the most important feature of an 'ideal' workplace, yet other factors rank higher on employees' priority list. 52% of workers say that access to the latest technology that enhances teamwork and collaboration is the workplace feature they value the most. ■

Edinburgh Council selects Jadu Central Gateway for secure remote access to intranet

Jadu has partnered with CGI and the City of Edinburgh Council to develop Jadu Central Gateway, a new intranet publishing platform that provides secure access to the council's intranet to frontline workers.

The platform addresses an issue faced by frontline employees who don't have regular access to the council's intranet, which limits their ability to access important internal communications, policies, guidance, and support, as well as information on pay, benefits, and wellbeing initiatives.

"This platform will provide access to a host of support documentation and guidance to all of our previously digitally excluded frontline employees. By creating a secure gateway to the intranet, Jadu Central Gateway ensures that all colleagues have access to the same information at the same time and is a significant step in our digital and accessibility ambitions. The platform reinforces our commitments to engagement and empowerment of colleagues, and to continue transforming services," said Cammie Day, council leader of The City of Edinburgh Council.

The Jadu Central Gateway platform also supports the Scottish government's 'A changing nation: how Scotland will thrive in a digital world' strategy, including the 'No-one Left Behind' theme, focusing on digital inclusion, accessibility and participation.

"This is an important project that will allow us to provide all frontline workers with secure access to important information and services. Jadu Central Gateway will provide employees with access to information they need to do their jobs more effectively and is a great example of how Edinburgh is leading digital innovation that can support their employees," said Tara McGeehan, president, CGI in the UK and Australia.

"We're solving a real problem for large organisations with a distributed workforce. What happens when frontline workers, contractors and remote teams cannot access internal policies and digital services, because they do not have a corporate email address?" asks said Suraj Kika, CEO of Jadu.

"Jadu Central Gateway solves this by enabling secure access to important content and digital services critical to supporting these roles. We're thrilled to be partnering with CGI to deliver this important initiative for the City of Edinburgh Council," outlines Kika. ■

GOSH's new Mind Palace supports clinical care

Great Ormond Street Hospital (GOSH), one of the world's leading children's hospitals, has furthered its collaboration with Hyland, a leading content services provider, by creating Mind Palace, a new customised solution that expands its Hyland Healthcare product suite. Mind Palace is designed to capture and manage clinical guidelines, policies and procedures that integrate with Hyland's OnBase platform.

To provide strong support for clinical care and the practice of medicine, searching and locating multiple documents in a hospital's digital footprint can be challenging, especially if real-time access is needed. Mind Palace serves as a knowledge base for staff that addresses these problems with faceted navigation, conversational search, natural language support and other intuitive features to enhance clinical productivity and patient outcomes.

"At GOSH, we care for children and young people with the most complex and serious health conditions and their care can span across many specialty areas," said Shankar Sridharan, chief clinical information officer at GOSH. "For our staff to deliver gold-standard care and we need secure, easy and rapid access to information within vast clinical guidelines. The Mind Palace knowledge base acts as a complimentary force to our electronic health record and will enable us to deliver better care." ■

Government targets cyber talent shortage, sees 3,600 applicants

The Department for Science, Innovation, and Technology's plans to build a thriving tech workforce and secure the resilience of the future digital economy is taking off with more than 3,600 applications to the government's Upskill in Cyber programme.

Aimed at people from a non-cyber background and delivered in partnership with the SANS Institute, the scheme is the latest in a series of ambitious programmes delivered through the government's £2.6 billion National Cyber Strategy. Almost half of the applications were submitted by women, and more than 50% coming from people based outside London and the South East.

"The UK's cyber sector is growing exponentially. In just 12 months we've seen our 58,000 strong workforce jump by 10%, and ensuring we can maintain a steady supply of diverse, highly-skilled professionals is vital to meet the needs of our growing digital economy," said minister for AI and intellectual property, Viscount Camrose.

Cyber skills are in huge demand across the economy. Last year's cyber security skills in the UK labour market report found that 51% of businesses have a basic cyber skills gap, with an average of 21,600 new recruits needed every year to meet demand in the cyber sector. ■

Word on the web...

Key lessons from the GoAnywhere attack

Paul Dant, senior director, cybersecurity strategy & research at Illumio

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

Drilling for data

David Shannon, head of hyperautomation, SAS UK & Ireland

Making sense of the data

Ever since the advent of big data in the 1990s, telecoms companies have been collecting more and more of it – keen to realise the value it can bring to every area of the business.

Data from a multitude of first and third-party sources, including customer interactions, device history, credit risk and networks, can all provide intelligence that drives cost efficiency, performance, and profitability in an increasingly competitive market.

What's more challenging is being able to make sense of this data quickly enough.

Take network operations, for example. It would be impossible for humans alone to make decisions like aligning latency, speed, and bandwidth for priority services, especially in the age of 5G and Internet of Things (IoT). Operators must be able to analyse increasingly large data volumes in real-time to support intelligent decision-making and guarantee Quality of Service (QoS) without relying on manual intervention.

The same is true of customer experience (CX), where a growing number of channels, services and offers create more data points in the customer journey. Elsewhere, the complexity of credit risk management and fraud today make it difficult to identify possible red flags, unless your data offers clear insights.

Identifying opportunities

Data silos are a common problem in large established telco companies, as they are in other sectors. While one team might think it's got to grip with its data, it could be missing out on opportunities to layer it with information from other departments to derive better insights.

Fraud analysts, for instance, could use marketing and customer service data to identify anomalies because perpetrators often behave very differently to legitimate customers when browsing products online.

A cloud-based analytics platform, with a scalable architecture, enables companies to easily bring together masses of structured and unstructured data in one place, and gain visibility across the entire organisation.

Advances in artificial intelligence (AI) and machine learning (ML) have made it possible to process data and highlight previously hidden insights that can be applied to real challenges. AI and ML can be layered onto and alongside existing automation workflows (enabling what Gartner has termed hyperautomation) to support faster and smarter decision-making.

In an uncertain world, the ability to collect and act on new data is critical. The current cost of living usually means that credit risk and fraud goes up and failing to respond quickly enough could be extremely damaging for a company.

Hyperautomation helps companies to develop highly accurate risk models that combine classical and AI techniques (like text analysis, and image recognition), and reduce the time it takes to develop and deploy models from months to just minutes. Similarly, when it comes to fraud, companies can draw on more first and third-party sources to successfully identify outliers and links between fraudsters.

Intelligent decision-making

It goes without saying that intelligent decision-making depends on the quality of the data being used as well as the quantity. Cleansing data can feel like an enormous challenge as companies amass more and more, but there are readily available tools that allow users to correct non-standard and duplicate data records, as well as integrate data and identify individuals from multiple sources, even if the relationships are incomplete.

Just as important in the highly regulated telco industry is being able to manage sensitive and personally identifiable information (PII) in compliance with privacy and data protection laws, such as the GDPR.

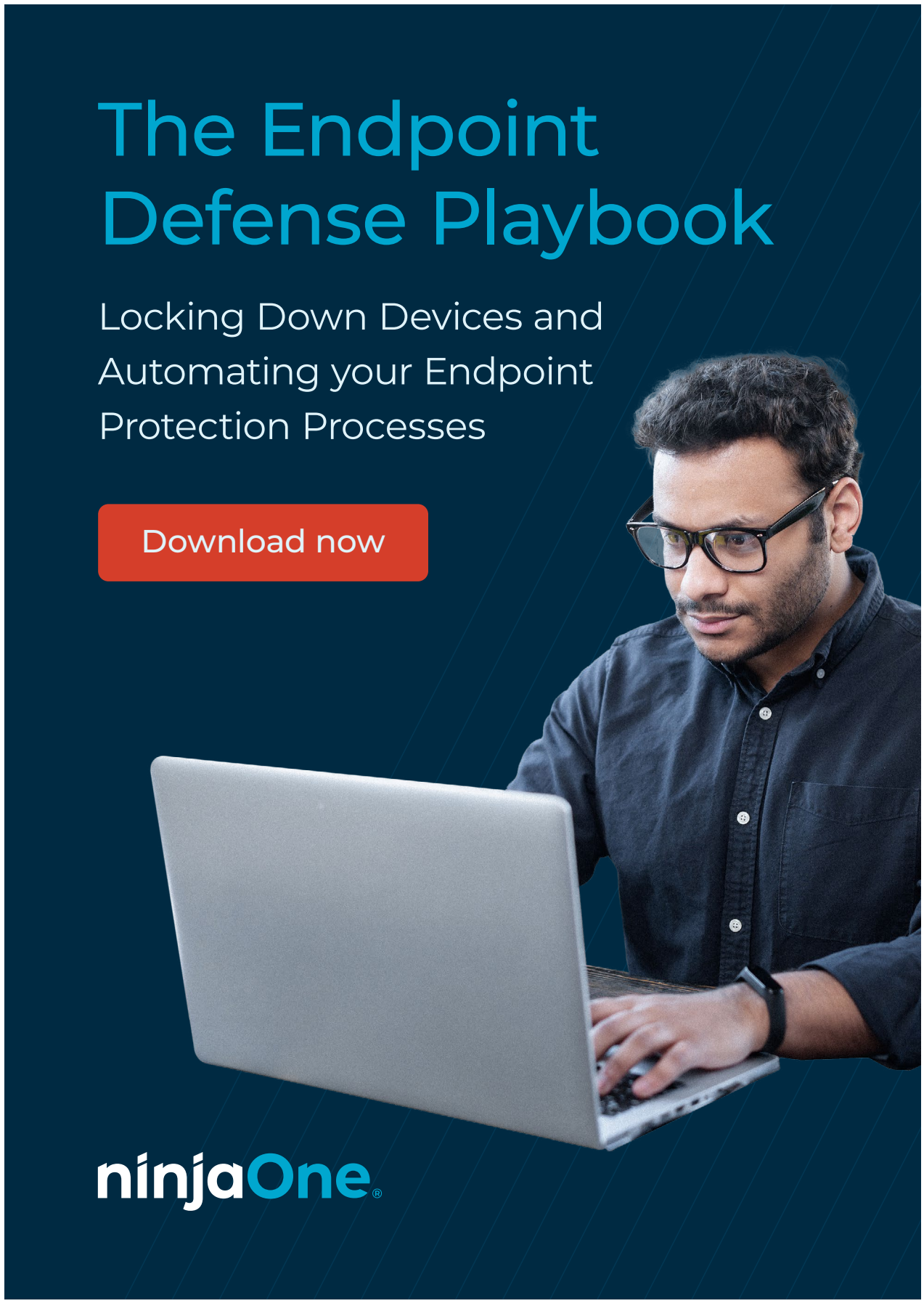
Data governance is a key focus at SAS – and we work closely with organisations to deliver solutions that enable them to set and enforce policies, and make sure highly-sensitive data is quickly identified and stored securely.

The technologies powering AI and ML are advancing all the time, removing previous constraints around data management, and helping telcos to innovate and remain competitive.

They also open up new opportunities to diversify into the growing B2B market, as IoT technologies become widely used in often-critical industries like energy and manufacturing.

On oil and gas rigs, for example, equipment can be fitted with sensors to automatically monitor performance and predict when maintenance will be needed in real-time. All this depends on a network that delivers low latency, high speed and the bandwidth to manage large amounts of data, which in turn depends on network analytics.

Thanks to low-code/no-code platforms, these tools are now within reach of non-technical employees – what we at SAS call the 'democratisation of analytics.' As well as removing the technical constraints to data analysis, empowering everyone to use AI/ML tools reduces the burden on those with in-demand data skills. This allows experts, whether they be in network operations, marketing, fraud, or credit risk, to build models that solve their specific challenges. ■



Deception technologies offer enhanced threat hunting capability

Mark Oakton, CEO/CISO, Infosec Partners

Cyber-attacks are undoubtedly becoming more sophisticated, more widespread and are proving to be more difficult to detect and defend against using traditional reactive security controls. This is forcing security teams to look for and deploy smarter threat hunting tools as a more proactive approach to protecting their network infrastructure and frustrate would be hackers.

Typically, the first that the SOC knows about an attack is when it is already in progress. If they are lucky their security platform will have done its job and blocked the attacker from breaching the first line of defence, lighting up their dashboards with alerts. However, if they are not so lucky, they are more likely to be dealing with a damage limitation situation and the consequences of unauthorised access to sensitive and valuable assets.

In recent years a new approach to cybersecurity has emerged that gives security teams the proactive tools needed to get ahead of the attackers and enhance traditional threat hunting methodologies, potentially saving expensive resources such as eliminating the time spent investigating false positives. Using advanced deception techniques designed to divert hackers away from live production environments to a decoy attack surface these tools can detect the typical tell-tale signs of an attack early in the planning and preparation stage such as attempts to access user directories and unusual lateral movements between systems.

businesses and public sector bodies?

Whilst there are signs that more companies are looking at introducing a deception-based approach to cybersecurity, and most leading analysts are forecasting significant growth over the next 3 to 5 years, there are still some challenges that are restricting the rate of adoption of the technology particularly among the smaller businesses. One of the major obstacles to more widespread deployment is that to be fully effective the technology needs to be closely managed and monitored by a dedicated team of security experts, which in addition to being a prohibitively expensive resource for most IT budgets, are also in short supply.

As with all cyber control frameworks there is an army of hackers continually working on ways of circumventing them by firstly identifying and then bypassing the decoys, which means that the SOC needs to be equally creative to ensure that the systems are obfuscated enough to delay detection long enough to give away their presence in the network as well as their motivation and intended targets to enable timely mitigating actions to be taken. In essence this means engaging with the attackers in real-time by changing elements of the decoy environment to create doubt and confusion so that they ultimately give up and move on - leaving behind useful information about themselves in the process.

To be able to operate at this level it requires a high level of expertise and experience, which is best delivered

"There is an army of hackers continually working on ways of circumventing them by firstly identifying and then bypassing the decoys, which means that the SOC needs to be equally creative."

The objective of deploying any security controls is to protect against all unauthorized access, and deception technology can be a useful added defensive layer to provide an early warning of an imminent attack or evidence of malicious activity already in progress, diverting the attacker to fake data and credentials to protect the enterprise's real assets.

Deception technology can also provide an effective research tool function. By analyzing how cyber criminals break the security perimeter and attempt to steal what they believe to be legitimate data, security analysts can study their behavior in depth such as recording the movements of malicious actors from initial contact through to interaction with the decoy. A server logs and monitors all vectors used throughout the attack, providing valuable data that can help the IT team strengthen security and prevent similar attacks from happening in the future.

Given the obvious benefits these relatively low cost and easy to deploy deception technologies can deliver for security teams it raises the question of why are these tools not more widely deployed by more businesses by transferring responsibility for the management of the technology to a dedicated security service supplier.

A professional managed deception technology service will enable enterprises to take full advantage of all the features and functionality it has to offer and ensure that it is correctly configured in line with the organisation's network infrastructure and existing security controls and can be monitored on a 24/7 basis by specialist security engineers, enabling a rapid response to the first signs of malicious activity.

For enterprises as well as small businesses deception technology changes the dynamic between themselves and their attacker putting them more in control of their network security and changing from a traditional defensive security posture to a more advantageous position that puts the hacker on the back foot. As such it can benefit any size organisation, regardless of the complexity of the network environment working together with existing security controls to minimise the chances of a preliminary attack turning into a serious breach. ■

Edge vs cloud? Don't believe it – they both need secure remote access

Alan Stewart-Brown, VP EMEA, Opengear

The much-touted death-match between edge and cloud computing for the future of global IT infrastructure is almost entirely hype. The reality is that they serve different purposes, and each will thrive.

It is likely that centralised cloud computing will continue as the standard model of IT delivery for the foreseeable future. Research company MarketsandMarkets expects the global cloud computing market to grow from US$545.8 billion in 2022, to US$1,240.9 billion by 2027, a compound annual growth rate (CAGR) of 17.9%.

However, new data-hungry applications demand an architecture that is built to support a distributed infrastructure – and that is what has sparked the new age of edge computing. In some ways, this is a response to the shortcomings of the cloud model, especially when it comes to latency and limited bandwidth when transferring high volumes of data.

Edge computing is great at processing time-sensitive data and connecting remote locations. It works well with dispersed workforces, bringing critical data 'nearer' to those needing to use it. Being connected to an edge data centre boosts reliability of access, security and productivity. It also addresses important data sovereignty and compliance requirements, keeping data inside borders without loss of performance.

There's no doubt that COVID-19 boosted edge computing through working from home policies, the growth of video streaming, and a rise in online gaming. A recent report covering edge computing trend analysis by components, applications, industry vertical and segment forecast, suggests the size of the global edge computing market should reach $155.90 billion by 2030, achieving compound annual growth of 39%.

Identifying potential points of weakness

Complementary rather than competitive, cloud and edge will thrive as data volumes grow. Yet, each is also vulnerable to cyber-threats. Cloud computing is centralised and susceptible to direct denial of service (DDoS) attacks and outages. Data breaches of multiple kinds are commonplace. An Ermetic-commissioned IDC state of cloud security survey, from 2021, revealed somewhat shockingly, that 98% of companies surveyed experienced at least one cloud data breach in the previous 18 months – a significant increase from 79% in the previous survey.

Edge, by contrast, is vulnerable because of the increasing demand for faster, more efficient services exerts more forces on distributed IT networks, increasing the likelihood of outages. Edge locations tend to have less built-in redundancy, and no on-site engineers, which gives them less resilience than traditional data centre locations.

This new world of cloud and edge will require organisations to rethink how they manage networks to continue delivering the always-on uptime that customers expect.

New thinking about resilience

There is a need for organisations and service providers to engage proactive monitoring and alerting to networks without having to send an engineer to the site.

Failover to Cellular (F2C) technology, which is part of this approach, provides continued internet connectivity for remote LANs and equipment over high-speed 4G Long Term Evolution (LTE), when the primary link is unavailable. Easily integrating with existing IT systems and network infrastructure, F2C restores WAN connectivity without a human being needing to step in.

Organisations are also using a combination of automation and network operations (NetOps) for zero touch provisioning of their smart OOB devices. In effect this provisions the smart OOB network and has it up-and-running without the risk of human error. Often, they will want to 'zero touch provision' their own devices. They will also want to use this technology for the orchestration of maintenance tasks and to automate remediation should equipment fail, or another technical problem crop up.

Organisations can ship new or replacement equipment to the location and employ Smart OOB to restore the site using a secure cellular connection. This enables remote provisioning and configuration of the equipment in-situ without having to send a skilled network engineer to what may be a remote site.

Employing these technologies and methods can deliver huge cost savings for companies implementing new edge deployments, especially when they are trying to move swiftly into multiple territories. If, after a deployment, a problem develops that results in a loss of connectivity to the production network, and it is one the organisation cannot resolve immediately, business continuity is nevertheless maintained. The organisation continues to transmit any mission-critical network traffic across the secure OOB LTE cellular connection.

Pairing smart Out of Band and the latest NetOps automation principles will ensure businesses achieve the always-on access necessary for network resilience. This is the level of resilience required to make cloud and edge deployments the unqualified successes they should be. ■

Register for Networking+

Matt Seaton

John Hall

Steve O'Brien

Charlie Stace

Roundtable: Are all colocation data centres created equal?

With the colocation data centre market booming, how can enterprises distinguish between the 'top notch' and the 'just ok'?

What should a user expect from a top-quality colocation data centre (DC)?

Matt Seaton, director, Netwise: A DC is all about providing a high uptime environment to critical IT services, so a natural focus should always be on the resilience of the core infrastructure like power, cooling, and connectivity. Any top-quality facility operator will also give focus to supplementary services, such as support and on-site amenities.

John Hall, managing director-colocation, Proximity Data Centres: The DC should have state-of-the-art infrastructure with redundant power systems, backup generators, multiple network carriers for diverse connectivity, advanced cooling systems, remote hands services, and physical security measures like biometric access controls and surveillance systems to protect infrastructure and data. It is important that this is a truly diverse infrastructure as regular maintenance is vital to ensure high availability: the facility should provide a highly reliable and redundant network infrastructure to ensure maximum uptime. This includes redundant power feeds, backup systems, and multiple network connections to minimise the risk of downtime.

Steve O'Brien, managing director, cloud, Redcentric: It's important to look at the features that provide added value. Sustainability is a critical issue, so features like immersion cooling can help to provide higher levels of energy efficiency. Robust backup and resilience plans should be expected from a top-quality colocation DC; even the largest hyperscalers have faced issues.

Charlie Stace, solutions architect, iomart: A user should expect robust, reliable, and redundant infrastructure, including, power, cooling, fire suppression and physical security. It's important that a DC has redundancy in each area to ensure that in the event of failure the DC continues to run smoothly. Features such as 24/7 physical security, monitoring, biometric access controls, and video surveillance are necessary. The DC should have a multiple carrier neutral network provider available to ensure clients have high-speed low latency connections. SLAs should cover response times for technical support, guarantees on power and network. These should also include schedules for maintenance. Compliance and certifications are also an important consideration.

What makes one colocation DC better than the next?

John Hall: As well as features such as the M&E infrastructure and connectivity, the most important factor is the team that is responsible for the day-to-day management. Do they have the experience and expertise as well as the 'can do' attitude to really understand client needs? Geographic location is also important as your team will probably need to visit the site.

Matt Seaton: Given the well-established tiering system for quickly identifying a DC's redundancy level, it should be simple to categorise groups of facilities together, which should all be of a comparable technical standard. It's everything that sits beyond this, at each level of operational standard, that sets one facility apart from the next. Do they offer 24x7 support and access? Is the facility well-maintained? Are they able to demonstrate the underlying technology? Do they have on-site amenities? Is the facility well-located? Are there dry loading capabilities? Do they have a delivery handling function?

Charlie Stace: Uptime and reliability are critical. Look for DCs with a proven history of minimal downtime, investigate how power is made resilient, and how long the facility can run with loss of power from the grid. The diversity and quality of the network connectivity also plays a significant role; look for DCs with Tier 1 carriers and ISPs. DCs with good access to major internet exchanges and content delivery networks offer improved performance and efficient data transfer. DCs should also be able to recover from disaster easily; look out for backup power systems (multiple generators), UPS, and diverse physical routes into the DC for both power and connectivity.

Steve O'Brien: This varies because of the differing needs of organisations and their specific digital transformation goals. If data sovereignty is the key priority, for example, then that will be the differentiating factor between one DC and the next.

What should potential users look to avoid?

Steve O'Brien: An absence of physical security safeguards and cybersecurity measures could indicate that a supplier doesn't prioritise security, which is critical for protecting sovereign data.

John Hall: Look at the team and see how they understand your requirements. Have they taken the time and effort to understand your needs and provide a solution to satisfy them 100%? Have they given good advice and discussed your current and future requirements? If not, then walk away.

Charlie Stace: You want to see as much resilience, and reliability as possible in most cases, however there could be some cost advantages in finding lower grade DCs if your requirements are not as critical.

Matt Seaton: Any visual clues during a tour that a site may not be well looked after are a red flag - a top-quality DC should always be extremely well presented. Beyond this, one of the biggest things to look at will be the financial stability of the company.

How big an impact does pricing have on quality?

Charlie Stace: It's important to remember that colocation is in a competitive market - pricing does not always have a significant impact on quality or service. That said, it's not unusual to find the top Tier DCs charging more.

Matt Seaton: As with most things, you do generally get what you pay for, and while some operators do unfairly leverage this based on their brand equity, for the most part, the very best facility operators will be positioned further up the pricing table. Designing, building, and running world-class DCs doesn't come cheap, and while the best DCs in the world do offer exceptional value, you can expect to pay a little more for that peace of mind. The race to the bottom on pricing is simply not conducive to operating a top-quality DC in the long-term, so if you see pricing that's too good to be true, it probably is.

John Hall: There are four broad areas of costs associated with DC services – setup costs for the initial installation; rental of the area used (rack footprint); power consumed; and connectivity. Power costs have been much discussed in the press and are important, but the cost of the rack footprint rental can vary considerably across the UK.

Steve O'Brien: Due to the current high costs of energy, many DCs have increased prices and mitigated passing on costs to customers to stay in business. Location matters and DCs located in high areas of energy demand will have to pass on those costs, making their services less value for money. It's worth examining how a given DC incurs costs and as a result, the impact that it has on quality. ■

Modern network optimisation

Network optimisation has never been as vital as it is today with the evolution of dispersed, hybrid working practises in the post-pandemic era. Amy Saunders asks network experts their thoughts on optimisation in 2023

Today's businesses are increasingly operational 24/7 because of a hybrid/dispersed workforce that needs to be able to work on any application at any time day or night, anywhere in the world. Accordingly, network optimisation is vital to meet the growing demands of digital transformation; enable seamless remote work; ensure data security; enhance user experiences; achieve cost efficiencies; and prepare for future technological advancements.

Network optimisation has always been important, but perhaps now more than ever as IT departments are making more strategic decisions. "Their networks have become increasingly complex and costly whilst budgets are being squeezed even harder, so the need for cost optimisation is critical," explains Martin Saunders, product and marketing director, Highlight.

Enterprises today are focused on operational agility to drive digital transformation, enable flexible working models, and adopt cloud resources from multiple cloud providers, but traditional wide-area-networks (WANs) were not architected for these use cases – from large scale cloud/multi-cloud usage - to a workforce that is largely remote with the need to be connected anywhere, anytime, says Darren Parkes, country practice leader, network & edge, Kyndryl. "Legacy networks also do not meet the security requirements required for these new digital paradigms."

The evolution of technology continues at a rapid pace, with the emergence of 5G, edge computing, IoT, and AI-driven applications. Network optimisation is essential to prepare networks for these advancements, ensuring they can handle the increased data traffic, low-latency requirements, and complex network architectures.

How important is visibility?

Visibility is a critical aspect of network optimisation, providing real-time insights into the performance and behaviour of network components, applications, and traffic flows; effective security monitoring and threat detection; an understanding of how applications and services utilise network resources to enable performance optimisation and implement quality of service (QoS); the ability to optimise capacity planning and resource allocation, for the present and the future; and a way for the enterprise to monitor and audit network activities to meet compliance.

"Visibility is a critical aspect of network optimisation and without it, it is difficult to understand how networks behave and in turn, how best to optimise them," opines Alan Hayward, sales & marketing manager at SEH Technology. "Seeing is believing that optimisation can help to spot issues such as bandwidth problems or security threats before they have a real impact on a network. Without visibility, optimisation becomes harder to successfully achieve, especially with data volumes increasing exponentially."

Without visibility, organisations tend to over-build in terms of capacity to be safe, according to Saunders: "as an example, a secondary school recently moved to a policy where everyone is using Chromebooks. Their IT provider advised that they needed fast internet since everyone would be online and recommended a Gigabit Ethernet service. However, when the school used the Highlight Service Assurance Platform to understand usage in real time, they could see their peak usage was only ever 25Mb."

However, while visibility is a key element, it is not the only one. Network optimisation encompasses multiple factors, and the importance of each can vary depending on the enterprise's specific goals and requirements.

"Visibility is not necessarily the most important, but it is certainly critical," adds Saunders. "To understand what you need from a network, you need to know what users are using today, how it is being used and for what purpose. Visibility is the starting point to creating a strategic plan."

Bridging the communications gap

Many of today's enterprises have a centrally managed network operations centre, and users often find it difficult to communicate their issues in an understandable way to those up the chain, resulting in miscommunication.

"It is important to remember that 95% of network users are in non-technical roles," explains Saunders. "This includes those who are in management and technical support roles. If you can help them to understand what is happening on the network and make the right decisions, you can minimise the time spent by experienced and expensive engineers

Register for Networking+

fixing problems."

So how can vendors and integrators help non-technical users articulate their problems and needs?

"Vendors and integrators can help non-technical network users by assuming that they know little about how to articulate problems and by trying to gauge the level of understanding that the end-user has," outlines Hayward. "Cutting out the jargon helps users to be on the same page and removes the technical terminology which can be daunting for non-technical roles. It's all about putting non-technical users at ease without overwhelming them with technical jargon and complex terminology."

Simplifying technical explanations is essential to enable effective communications between technical and non-technical users on networking challenges. Offering user-friendly tools and interfaces like visual dashboards or step-by-step troubleshooting guides is another route to empowering network users to self-diagnose and report network issues more effectively.

One size fits all?

When it comes to network optimisation, every enterprise has unique requirements for infrastructure, applications, and business goals: there is no 'one size fits all.'

"One solution doesn't fit all, and IT managers need to choose a solution that works for them and their needs," says Hayward. "Once a solution has been chosen it then needs to be monitored to see how it works in practice. While a solution may look good on paper, in practice it might not work exactly as intended. Without monitoring, network optimisation won't achieve all the possible benefits."

The optimal network optimisation solution will vary significantly depending on factors such as the enterprise size, industry, network architecture, traffic patterns, and performance objectives. Moreover, different organisations may prioritise different aspects of network optimisation based on their specific needs. A large enterprise with geographically dispersed offices may require solutions that focus on WAN optimisation and traffic management, while a small startup heavily reliant on cloud services may prioritise solutions that optimise cloud connectivity and application performance.

It is essential for enterprises to thoroughly assess their requirements, conduct proper analysis and testing, and consult with network experts or vendors to determine the most suitable network optimisation solution for their specific needs. Customising the solution to align with goals, network infrastructure, and performance requirements is crucial for achieving optimal results.

"It is important not to be drawn into what is being hyped. We have encountered lots of examples of SD-WAN regret, where companies have jumped on a technology before really understanding how it needs to be done," says Saunders. "Properly understand what you need, where you are going and ensure that optimisation is part of the strategy first before making long standing decisions about vendors and technologies."

Choosing the right solution

IT managers must consider several important factors to ensure they choose the right network optimisation solution for their enterprise's specific needs, such as scalability and flexibility; security capabilities; ease of deployment and management; performance improvement; cost effectiveness; analytics and reporting; and vendor support and reputation.

"Some of the most important considerations are current remote site performance, requirements for latency sensitive applications and efficient and secure network access," says Jeremy Reese, WAN networking product line leader, Kyndryl. "IT modernisations can fail if inventory records of legacy infrastructure isn't very good. Doing the necessary research to understand what's needed often requires a lot of additional resources — and many companies lack resources to allocate to the effort."

For Hayward, it's about choosing one that fits the problem, taking into account the resources available to an IT manager, as well as one that's simple to use: "SaaS spending is a key area of concern for IT managers and network optimisation solutions need to provide value and be capable of factoring in network requirements rather than just becoming another SaaS solution sitting on the shelf, especially important in a rapidly developing emerging technology-filled world."

When choosing an optimisation solution, IT managers should also beware of avoiding pitfalls like compatibility, which can lead to integration challenges and disruptions.

From ignoring the critical aspects of an optimisation solution outlined above, to failing to conduct a thorough proof-of-concept (PoC) or trial period to evaluate its performance in a real-world environment and forgetting about long-term needs – resulting in frequent replacements or additional investments – IT managers must keep their eyes on the ball.

"With so many pitfalls, the best option is to try before you buy," asserts Saunders. "This means you don't get stuck in a particular technical or vendor direction. Service providers often have wide access to different vendors, as a result they are more vendor-agnostic and can provide user references for the different technologies."

Moreover, effective network optimisation is not a 'one-and-done': "it is a continual ongoing process where you should always be moving in the right direction based on data," explains Saunders. "This is where having one clear view of how all network elements are performing together is invaluable.". ■

Using USB devices while working remotely?

It works in fact securely with our utnserver Pro!

The use of USB devices when working from home and at other remote workplaces is currently important – and will remain so in the future.

Nevertheless, the security of the data should continue to be guaranteed.

The next generation of our USB device servers implements this challenge in several ways!

Our utnserver Pro convinces with brand new product features:

- Complete solution: complete hardware and software package
- Quickly installed, easy to use
- Improved usability

utnserver Pro

Made in Germany

Supported devices:

External hard disc · Flash drive · Scanners · Gauges · Medical · RDX- removable discs · Multifunction Pheripherals · Camera · Telephone systems

So, are you prepared for the future?
www.seh-technology.com/uk

SEH

IoT and the road to long-term water security

Climate instability combined with an expanding population and escalating levels of per capita consumption are creating unsustainable pressure both on water resources and an overstretched supply network. Yet, without any insight into where leaks occur or how consumer behaviour affects consumption, how can water companies meet the government's ambitious plans to reduce usage? Alex Barter, manging director, B4T, and Gareth Mitchell, key account manager UK, Heliot explain why smart metering is key to creating a water secure future.

The UK has a serious water problem. 3 billion litres of water - over a fifth of the total supply - are lost to leakage every single day. Not only is this a terrible waste of a valuable resource, but when 3% of the UK's energy consumption is required to move water around the country, the full environmental impact of leakage is even more significant.

Nonetheless, water awareness remains low. People rail against the hosepipe bans and complain about the abstraction that depletes rivers across the country. However, consumers are a key contributor to wasted water. From dripping taps and faulty ballcocks to more serious leaks between the home and the street supply, 25% of UK homes are affected by leakage of a litre per hour.

Furthermore, at 140 litres per day, the UK's per capita water usage figures are far higher than in more water conscious countries, such as the Netherlands, where usage is 107 litres per day. Be that as it may, without any insight into how much water they are using and no understanding of the financial or environmental cost, consumer behaviour will not change.

Identifying leaks

While the highly regulated water industry is under pressure to address leakage – and, because meters are in place for just a fraction of the UK's residential and smaller commercial properties, water companies are blind to the locations of leaks. What is customer side? What is network side? Where should investment be prioritised? How can consumers be encouraged to change their water consumption behaviour?

If the industry is to achieve the leakage reduction goals proposed by OFWAT, metering is imperative. How else will companies identify the 20% of houses that use 80% of water? Or target the 1% of worse performing properties responsible for 80% of all leakage? The ability to identify and address the biggest problem areas will deliver a very rapid improvement in leakage performance.

Yet today just a fraction of the UK's business and consumer premises are metered. Even then these meters are typically not smart, requiring manual data collection. The problem has been the cost and complexity associated with deploying proprietary metering technologies at scale. How can companies deploy meters to millions of households? How can the sensors pick up information when the meters are buried underground, typically beneath metal covers which can block access to 4G, 5G or WiFi? How can the information be collected, collated, and analysed to deliver immediate, usable insight?

IoT value proposition

Proprietary technology has constrained smart metering not only in the UK. In both Slovenia and Switzerland, where water companies have a smaller customer base, meters are ubiquitous – but not smart. Every company relies on a fleet of engineers to drive around and manually take water readings. In addition to the cost, companies lack the real time insight into water usage required to quickly identify and repair leaking pipes.

The arrival of the Internet of Things (IoT) and highly reliable, low power networks have fundamentally transformed the cost/ benefit model for smart water metering. Sensors can collect water usage in real-time. Data can be transmitted and transformed using machine learning to provide unprecedented insight – from highlighting the biggest areas of leakage to supporting predictive maintenance.

There is also no need to rip out and replace the existing infrastructure. Current metering solutions can be upcycled into connected assets at a fraction of the cost to replace and without creating any landfill. With batteries that last up to 15 years, companies can deploy once and gain long term benefit. For water companies in Slovenia and Switzerland, this approach is already proving compelling. Engineers can be redeployed from meter reading to added value activities, and the existing asset estate can be reused to create an intelligent, smart meter network that delivers real-time alerts into leakage incidents.

Conclusion

No one is underestimating the scale of the challenge facing UK companies. Over 260,000 miles of water mains – many ancient. A population with limited awareness of the value of water. But if further action is not taken, between 2025 and 2050 the UK will need more than 3.4 billion additional litres per day to meet future demand for public water supply – and that is not financially or environmentally sustainable.

For water companies, the ability to identify the sources of leaks in real time is amazingly powerful. It will enable rapid response to problems, minimising the amount of wasted water and support far more targeted investment. For consumers, better understanding of their water usage habits will be vital to encourage individuals to change their behaviour and reduce day to day consumption. Together, these changes will be essential to achieving a secure water future. ■

Register for Networking+

Enhancing IT efficiency for Canterbury Christ Church University

Canterbury Christ Church University is a vital source of training for healthcare and teaching professionals. The university has three campuses across southern England, and partnerships with other academic institutions around the UK and the world, and so it needs to host high performance software to support their programmes at all levels.

Its partnership with the University of Kent to establish the region's first ever medical school required that Kent and Medway Medical School students could access both institutions systems, including being able to use the Canterbury Christ Church desktop service from campus and several NHS locations. The university also wanted to provide academic and professional service staff with hybrid work models, at a time when the country was in lockdown due to COVID-19. To achieve this, the University needed to convert on-premises remote desktop services (RDS) to enable access to campus desktops across all its sites.

The IT department initially implemented generic student desktops in 2020 to ensure access to university resources. However, the maintenance and scaling necessary for so many users provided significant challenges for the IT department.

"The University needed to implement a cloud first strategy to lower costs and scale to accommodate a hybrid model," said Dave Haliwood, platform and systems manager at Canterbury Christ Church University. "On-prem alternatives required too much specific expertise to maintain and simply were not flexible enough to meet our needs."

Tailoring virtual desktops

When the initial RDS licences came up for renewal, Haliwood turned to Microsoft's Azure Virtual Desktop (AVD) to help enable the university's hybrid model and make it easier for the IT team to create host pools for every department. This improved functionality, but the university's IT team still needed something that offered a complete automation package beyond the Azure admin portal.

Accordingly, the university imported eight host pools from native Azure into Nerdio Manager for Enterprise, resulting in an immediate ease of management and scaling.

"The Nerdio technology made it much easier for my team to build and manage host pools while still providing a great service to our users," said Haliwood. "It is simple compared to the complexities of native Azure but still provides IT with all the options they need to make customised updates."

Improving efficiency

The university's IT team of 68 people needed a streamlined, automated management tool to power such a big and heterogeneous organisation, especially with its tight IT budgets. The native Azure solution proved to be complicated, and Nerdio Manager for Enterprise helped to make the cloud environment immediately more manageable.

"A good example is The School of Engineering, Technology and Design," said Haliwood "Its host pool had particularly sophisticated requirements with the need to provision high-performance and with Nerdio Manager's auto-scaling features we immediately saved 70% through its compute and storage scaling, managing session hosts, reducing profile storage capacity."

The university's IT team is now able to use the Nerdio portal as an ad hoc service desk, allowing them to manage session hosts and individual sessions. This allows them to offer better experiences to users. Nerdio Manager for Enterprise ensures that updates can be made quickly in just two clicks, as the portal provides a single point of operation for all automation and AVD management.

Enhanced student and staff experiences

With Nerdio Manager for Enterprise, Canterbury Christ Church University has been able to increase the speed of AVD adoption across the organisation, while improving user experience.

"Nerdio made everything much easier and has enabled us to do more with AVD than we ever could natively," said Haliwood. "The automation and ease of use provides the team with much more flexibility, allowing us to create bespoke environments for specific departments while still keeping costs low and allowing for proper testing and rollout. Our users have never been happier with the experience."

While creating a new host pool used to take weeks, or months, with Nerdio Manager for Enterprise that same work takes less than a day. Nerdio's solutions helped the IT team to customise desktops and better serve the academics. Now the IT team no longer worries about capacity and has seen a significant decrease in IT support claims.

"Canterbury Christ Church University demonstrate the power Nerdio and Azure Virtual Desktop have to empower remote learning and enhance the modern student experience," said Tom Archer, regional sales manager, UK & Ireland. "Their ability to deliver a low-cost, high-performance route for accessing teaching and learning resources showcases this, it is a win-win-win for all involved." ■

Providing critical infrastructure for Ireland's education sector

HEAnet, the national education and research network for Ireland's education sector, serves more than one million users across the country. Its remote network infrastructure is crucial to connecting students, researchers, and staff to essential resources. The state-of-the-art network consists of several resilient layers that provide national coverage and connect their users to the rest of the world. For users across Ireland, it's crucial that HEAnet maintains comprehensive control of their critical remote infrastructure to prevent downtime.

With its existing out-of-band (OOB) solution reaching its end-of-life, HEAnet needed a replacement that could roll out to more than 50 remote sites. These point-of-presence (PoP) locations provided critical interconnectivity between sites; however, some of these PoPs were placed in extremely remote locations that were difficult to reach. On top of this challenge, HEAnet employed a limited number of technical resources, most of which were needed to uphold the organisation's four-hour service-level agreement (SLA).

HEAnet opted to outsource the job to an experienced managed services provider (MSP), aiming to maximise uptime and minimise time to resolution, which meant they required a solution that could: replace their existing OOB solution; provide centralised management and in-depth control; reduce infrastructure complexity; and provide resilience through LTE failover and high availability.

A truly open operating system

To lead the implementation, HEAnet chose Rahi Systems as its MSP.

Rahi deployed ZPE Systems' Nodegrid services router (SR) family of devices. One of the biggest reasons for choosing Nodegrid was that it provided a complete total cost of ownership (TCO) to HEAnet. Because of Nodegrid's hardware modularity and truly open, Linux-based Nodegrid OS, the TCO was clear from the start. This included hardware (with LTE cellular module), software, support, and warranty.

At its two large sites, HEAnet deployed the Nodegrid Net SR (NSR) complete with LTE cellular module for backup connectivity. With one NSR, it was able to replace both a console server and central access server at each location, while gaining cellular failover and additional switching capabilities. At the 50+ remote locations, it deployed the Nodegrid Gate SR (GSR) also with onboard LTE capabilities. This replaced a console server at each site while introducing additional serial connectivity. Running on all Nodegrid devices is a multi-core, x86 Intel CPU and the powerful Nodegrid OS. These allow for fast data speeds and responsive out-of-band management of all connected devices, which would prove critical to managing HEAnet's optical, MPLS, and IP infrastructure.

Rapid deployment with added resilience

The Nodegrid solution proved much faster to deploy than offerings from competing vendors. Whereas other solutions required a full day's worth of effort to bring sites online, Nodegrid could be set up in only a fraction of that time. Because Nodegrid supports true zero touch provisioning, it can automatically build entire environments in as little as 30 minutes. This allowed a single engineer to fully deploy and install two sites per day — including removing old kit, installing new kit, racking, stacking, and other proper installation protocols.

The NSR and GSR also come with plenty of serial interfaces, which allowed teams to connect critical routers, firewalls, fibre equipment, webcams, and rack PDUs to the consolidated solution. Both large sites ran parallel to each other to provide high availability and provided centralised console access to all 50+ distributed remote locations. HEAnet was also able to deploy an extra-stable VPN tunnel that dynamically follows available connections, for added resilience to downtime.

Nodegrid replaced HEAnet's existing OOB solution to give support teams centralised, in-depth management capabilities of all critical remote infrastructure. Nodegrid also reduced the hardware footprint to simplify deployment and operations, while providing a robust platform for serial connectivity, cellular failover, making sure the sites were never offline, and redundancy.

Because Nodegrid eliminated complexity by consolidating the hardware footprint and centralising OOB access, uptime became extremely resilient while resolution times were minimised. With only a single Nodegrid device at each location, teams could connect and gain access to a plethora of critical infrastructure, including routers, firewalls, fibre equipment, and PDUs. This drastically expanded the control of their OOB network, and Nodegrid's built-in LTE meant they didn't have to add additional devices and complexity to gain cellular backup.

More reliability was baked into the solution in the form of an extra-stable VPN tunnel. This dynamically changed to follow current available internet connections, keeping sites online regardless of provider interruptions and outages. With devices directly connected to the internet, HEAnet did not have to compromise on security. The vendor neutral Nodegrid OS enabled the deployment of its choice of solutions to keep infrastructure protected and includes a powerful virtualisation layer to accommodate changing future needs. ■

Industrial IoT Antenna Solutions must be *Flexible* enough to accommodate different wireless technologies, *Dependable* enough to offer continuous coverage and real-time data and *Tough* enough to withstand harsh weather or rough treatment.

STAY CONNECTED

Improve Your Network Connectivity!

INDUSTRIAL IOT

MobileMark antenna solutions

Mobile Mark Antenna Solutions designs and manufactures site, mobile, device, embedded, and covert antennas for 30 MHz – 9 GHz. Applications include GPS Tracking & Fleet Management, Mining, Cellular, 5G LTE, WiFi, ITS/V2X, Public Safety, Military and M2M. Engineering, customisation and bespoke design services are available.

Mobile Mark (Europe) Ltd
Tel: +44 1543 459555
www.mobilemark.com
Email: enquiries@mobilemarkeurope.com

Register for Networking+

The radio emissions problem and how to solve it

Charlie Bellsham, senior principal systems engineer, and Ciaran McCloskey, product line manager, Thales

The element of surprise and remaining undetected to the enemy has been central to the success of military combat throughout history.

Missions depend on not being seen. We often refer to the Seven S's (shine, shape, shadow, silhouette, spacing, signature, sudden movement) – the key ways in which troops are typically spotted, with survivability greatly enhanced if they can be managed effectively.

The consequences of detection can be fatal. Not only are lives at risk, but entire missions are potentially jeopardised if enemies are alerted to your presence and therefore able to respond, from deploying surveillance drones or troops, to carrying out precision attacks and indirect fire on a detected position.

Today, there are many tools and systems that enable visual, thermal and acoustic detection of dismounted soldiers, including day/night optic systems, thermal imagers and unattended acoustic and seismic ground sensors. And now, people can track radio emissions to identify where dismounted soldiers are.

The radio risk

A crucial part of a soldier's kit, radios have advanced their capabilities and greatly contribute to mission success. However, such enhancements have also brought with them a heightened risk of being detected.

Indeed, radio frequency (RF) signature is emerging as an increasingly reliable means of detecting, observing, and tracking the movement of troops.

This is because RF signatures can be picked up in almost any situation – day, night, in trees, while dug-in, in buildings, under cover, and in bad weather. Conversely, visual methods of tracking can be countered by being under cover and are hampered by extreme weather conditions, while thermal systems will not pick up signals of troops hiding in buildings.

And there are many products which perform RF detection in a variety of situations, spanning handheld and manpack devices, to larger pieces of equipment mounted on vehicles.

Between them, these systems carry a range of capabilities that enable users to gauge where soldiers are located or moving to, who they are and what their intent might be. Specifically, the systems carry out analysis of frequency bands to discover an operator's identity and use directional antenna to provide the origin of the transmission to pin down location, with the linking of two units allowing for accurate tracking and triangulation. Ongoing sampling and analysis of the information provided by RF detection systems provide further insight into speed and direction of movement which could be used to discover enemy intent.

Newer radios can be particularly prone to detection for a variety of reasons. Due to the integration of capabilities such as video transmission, they typically involve the use of more data which in turn demands wider-band radio devices that are easier to detect. This is because they occupy more of the radio spectrum, have higher duty cycles, and require greater amounts of power to achieve range.

Additionally, some modern military radios leverage commercial transceivers and waveforms which leave them particularly vulnerable to detection or jamming.

We are seeing the importance of RF detection play out in current warfare, not least in Ukraine where armies of a similar stature of technological capability are taking advantage of tracking technology to target troops to devastating effect.

How to reduce the likelihood of RF detection

Radios are and will continue to be a critical part of military operations, with their uses far outweighing the pitfalls, providing those pitfalls can, at least in part, be mitigated.

Indeed, while there will always be an inherent risk with using radio communications, there are several ways in which military setups can minimise the opportunity for their adversaries to make use of RF emissions.

Minimising transmission power, for example, will reduce the ability to be detected at range, while narrowing bandwidth will result in less spectrum usage which also reduces the probability of detection.

Consider the use of software defined radios (SDRs). These hold multiple waveforms, meaning a particular waveform with its own unique profiles and protections can be selected based on the level of risk in their location. They can also constantly hop frequencies to make it much harder to detect and track.

Behavioural actions can also help. These include minimising the time spent on air and lowering the duty cycle by reducing retransmissions.

Conflicts are defined by the technology that is leveraged in them. The humble radio, a staple of military kits for decades, is now a frontier of modern warfare that needs to be managed carefully to protect soldiers and increase the chance of mission success. Minimising the risk of detection via radio frequency emissions is therefore a critical consideration on today's battlefields. ■

Picking a wireless router? Focus on enterprise needs

Joshua Hodges, pre-sales engineer, TRENDnet

Selecting the best wireless router for an enterprise is a crucial decision that will have a big impact on your network. One must consider more than just the router that will be used, but how it will impact the entire network. In general, in addition to overall speed, security protocols, and a variety of other features, a business will want to look for a wireless router that supports VLANs, VPNs, and multi-WAN connections.

Here are the most important factors to consider when selecting a wireless router for your enterprise:

Network requirements: Consider your business's specific network needs and requirements when selecting a wireless. This includes the number of connected devices, the coverage area, and bandwidth requirements. Note that some network functions can be done by Ethernet switches and wireless access points on the network.

Wireless standards, speed, and performance: Routers with the latest wireless standards (such as 802.11ac/Wi-Fi 5 or 802.11ax/Wi-Fi 6) will have faster speeds, better wireless range, and improved performance compared to older wireless standards. However, depending on your needs and budget, you may be able to get by on a legacy model router.

Nonetheless, router speed and overall performance are important factors when choosing your business router. Depending on your network requirements, look for wireless routers that offer high data transfer rates, and multiple antennas for improved wireless signal strength.

Keep an eye out for advanced features such as beamforming or MU-MIMO that assist with more efficient data transmissions and enhanced range. Beamforming technology increases real-time performance by directing strong wireless signals to a specific location. MU-MIMO (Multi-User, Multiple-Input, Multiple-Output) technology processes multiple data streams simultaneously, increasing real-time WiFi performance when multiple devices access the network.

Security: Reliable network security is crucial for businesses, not only to protect company data, but data on customers and clients. Look for wireless routers with robust security features, such as the latest encryption protocols, VPN support, and built-in firewall. In some cases, you may want the ability to create an isolated guest network (although this can be accomplished by other means, e.g., VLANs and access points).

Management and monitoring: Router management and monitoring features allow businesses to control its network much more effectively. Management and monitoring of router resources helps to reduce network downtime, as well as identify network issues before they become critical problems.

Some features to consider that enhance network performance include traffic prioritisation or quality of service (QoS), and remote management. Traffic prioritisation, or QoS, assigns different levels of importance and bandwidth depending on the type of data packet(s). QoS intelligently prioritises voice, video, and other data traffic to improve network efficiency and overall performance.

Scalability: Choose a router that not only accommodates your business needs today, but one that can be scaled for future growth. In the future, you'll likely need to expand your bandwidth to support your business's, so consider routers that can handle a high number of connections simultaneously, or utilise mesh network technology for a simple, seamless coverage solution.

Reliability: Choosing a router from a reputable brand will give you peace of mind that it is reliable and durable. Take a look at the company's warranty and return policy in case of any issues or defects. Also, if choosing one, a business-grade router is designed to perform in more vigorous conditions than home or budget routers. They are designed to handle a high-degree of continuous usage, and reduce the chances of interruptions to the network.

Focus on your needs, performance reliability, security, and scalability. However, you may also want to consider your budget, and available support and services from the router manufacturer. Even if you find the perfect business-grade router, if it's not in your budget, it becomes a moot point. However, you should prioritise quality and performance over cost. And while the main factors and budget are important, the availability of reliable tech support and customer service (including the warranty) can be priceless.

Though not required, you may want to select a manufacturer that also offers a decent range of other networking solutions for future expansion considerations. Using products from the same brand should make changes and expansions more seamless.

And finally, learn from those with similar network requirements and experiences. Read product reviews from trusted sources, and seek out router recommendations from industry experts and colleagues. ■

PRODUCTS

ASUS' BRT-AC828 router, an ultra-fast AC2600-class dual-band 802.11ac wireless device with a four-transmit four-receive (4x4) antenna configuration, delivers all the networking features vital for enterprises.

ASUS AiRadar combines beamforming with the four external antennas for reliable, powerful and ultra-fast WiFi with combined speeds of up to 2534Mbps. For fast and resilient internet connectivity, BRT-AC828 features dual Gigabit WAN ports that offer up to 2Gbps aggregated bandwidth, with automatic failover in the case of interruption to one of the internet connections. Other business-focused features include an easy-to-configure secure WiFi portal for consumers, simplified device management using Device Grouping, and a RADIUS server for secure authentication and easy user administration.

The router enables fast and stable connections to multiple devices with excellent coverage. For complex office layouts, the powerful four-transmit, four-receive (4x4) MIMO design with four external antennas and fine-tuned power output ensures optimised reception for the best possible performance. Supporting up to 250 simultaneous WiFi connections, BRT-AC828 is suitable for heavy usage requirements, while the MU-MIMO technology allows multiple MU-MIMO-compatible clients to work at full speed.

Two physical 1Gbps WAN ports can deliver aggregated WAN bandwidth of up to 2Gbps for high-speed internet connectivity, and for non-stop internet access, these can also be configured as primary and secondary internet connections, with failover to the secondary connection if the primary fails. There is also the option to connect a 4G LTE dongle to the USB 3.0 port for use as a primary or secondary WAN, enhancing versatility.

The TP-Link Archer AX6000 next-gen WiFi router is one of the top-rated routers for enterprise this year.

It features dual-band WiFi speed boosted by 1024QAM to deliver high wireless speeds up to 5,952Mbps: 4,804Mbps (5GHz) and 1,148Mbps (2.4GHz). With one 2.5Gbps WAN port, eight gigabit LAN ports, and two USB 3.0 in Type A and Type C, the Archer AX6000 has excellent connectivity at hand.

OFDMA increases average throughput fourfold in high-density scenarios, compared with an 802.11ac standard router. Downlink and uplink MU-MIMO are both supported. The 1.8GHz quad-core CPU and two coprocessors eradicate latency and deliver stable performance, providing powerful processing for the enterprise.

Intelligent band steering directs clients to the less congested band and Airtime Fairness optimises the time usage, while set up takes just minutes via Bluetooth using the Tether app.

Finally, in-built security TP-Link HomeCare provides the whole network with advanced antimalware service powered by Trend Micro, delivering Antivirus, parental controls and quality of service (QoS).

Grandstream's latest products to market, GWN7062 and GWN7052, comprise dual-band WiFi routers with 2x2:2 MU-MIMO to support mesh networking, wired AP connections, VPN, advanced QoS, and powerful security features.

The GWN7062 is powered by WiFi 6 technology and provides WiFi speeds up to 1.77Gbps for up to 256 concurrent users, while the GWN7052 is powered by 802.11ac WiFi technology to provide speeds up to 1.27Gbps for up to 100 concurrent users. By providing accelerated WiFi speeds with strong security protection and advanced features, the GWN7062 and GWN7052 are ideal for SMEs.

The GWN7062 and GWN7052 both provide enterprise-grade security features to ensure secure WiFi and VPN access, including unique security certificates and random default passwords. These routers support VPN to allow remote employees to securely connect to the corporate network from home or branch offices. To ensure easy installation and management, they include a built-in controller embedded within the product's web user interface. TheGWN7062 and GWN7052 will also be supported by GWN.Cloud, Grandstream's upcoming free cloud Wi-Fi management platform. For home use, the routers can support bandwidth-demanding applications, including smart office and home automation, video conferences, web meetings, 4k Ultra HD video streaming, online gaming and more.

Synology's key product for the SME sector is the RT2600ac, a high-speed, security-focused router, which delivers robust performance with stable, uninterrupted wireless and wired connections for multiple users at the office or home.

The RT2600ac is powered by a 1.7GHz dual-core processor and comes with the latest 802.11ac Wave 2 certified radios featuring MU-MIMO support, so more devices can connect at higher speeds. To maximise network performance and user experience, together with Smart Connect, RT2600ac can intelligently optimise connection quality and balance devices on both 2.4GHz and 5GHz radios for maximum wireless speed and range. Dual WAN with 2.0Gbps combined bandwidth allows users to take advantage of two high speed fibre internet connections for load balancing plus failover.

Synology's RT2600ac router is powered by the Synology Router Manager (SRM) operating system, which offers professional-level networking tools. The Application Layer QoS (Quality of Service) makes it possible to monitor and control bandwidth consumption according to not only devices, but also individual applications. With advanced traffic control and application detection enabled, the hardware acceleration engine serves to maintain high performance and throughput for all connected devices. The RT2600ac is WiFi and DLNA Certified.

Moreover, with VPN Plus Server add-on package, RT2600ac can deliver client-free WebVPN in addition to minimal-setup, high performance Synology SSL VPN solutions.

Please meet...

Mark Yeeles, VP UK & Ireland, Schneider Electric

Which law would you most like to change and why?

One of the key areas I feel we could improve is to better educate our children about the power of working collaboratively and as part of a team.

Repivoting the educational system to teach children and young people vital skills to help them better prepare for all areas of work and help them recognise the valuable contributions that people from different backgrounds, and with different skill sets, can bring when seeking to achieve a specific goal or outcome. This is something I believe could lead to many tangible and positive outcomes for the country.

What was your big career break?

My real career break was deciding to take the plunge into the commercial world of sales. Until my mid-20s I was an engineer and technologist by trade, and then I decided to go into sales, which was from a career perspective the best decision I've ever made. My background in engineering and technology has also played a pivotal role in my effectiveness to understand customer challenges and a greater ability to empathise with customers.

In terms of a pivotal point in my career, however, this came when I joined Rockwell Automation as an account manager, and ever since, my career has fortunately been on a successful trajectory.

What did you want to be when you were growing up?

Top Gun was one of the most influential films of my teens, so I wanted to be a fighter pilot!

Fortunately, my dad recognised that I had a bit of interest in toys like electronic building kits, so he fostered this and when I was old enough took me to a local company's open evening – Perkins Engines (a partner of Caterpillar group) which gave me my first taste of the engineering and working world. After that, I was hooked, and my passion for industrial software and people emerged.

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

Well, I always think a dinner party for four would be a bit more fun.

First, I'd invite, Barack Obama to dine with me. I'd love to spend some time with that man! The way he handled himself throughout his tenure was quite phenomenal and he's a shining example of a truly inspirational leader. He also seems a genuinely nice guy with excellent values, which you can see through his relationship with his daughters and wife. It'd be fascinating to discuss the challenges he endured during his time in office, and how he convinced people to both trust his decisions and stick with a journey based on hope.

Second, I'd invite Winston Churchill and for similar reasons. I'd like to explore how he remained calm and rallied a team together when the country was under such serious pressure during various stages of the war.

Last but certainly not least, I'd like George Best to join us. As a footballer, he is one of the best who has ever played the game, he lived life to the full and was a character both on and off the pitch. I imagine he could take us on a decent night out after all those in-depth chats and would add an interesting dynamic to the table.

What's the greatest technological advancement in your lifetime?

The iPhone – there's no doubt that its innovation has changed the way in which we work, live, and interact as humans, fundamentally enabling people to connect better. It's also led to a plethora of technological innovations that have been created directly off the back of the technology, both in terms of hardware and software.

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

I'll try to narrow it down to three:

First, my parents always told me, just try your best and the outcome will be the outcome. That gave me the confidence to try new things and when I felt out of depth, ask what's the worst that can happen?

Second, a former leader once told me that it's so important to recognise that people within your team will always operate in different ways to you, so expect the unexpected all the time. When given an opportunity, most people will surprise you (pleasantly) and step-up to the plate.

Third, be clear about what you stand for and what you believe in - and ultimately be your authentic self. This is essential in any leadership role and will allow you to succeed.

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

After moving from the industrial sector into data centres, you could say I've just made the leap.

However, I'm fascinated by people and would love to work in the media - primarily to better understand insights into sporting personalities and the psychology behind their profession.

From a technology perspective, I'd also be interested in exploring new ways to encourage young people into our industry, as it really is such an exciting place to be! We are at the leading edge of technological innovation, which is rapidly changing everything about the way we live and work, so it's important that we democratise the sector to open up new opportunities for a more diverse workforce and attract more people from different backgrounds. ■