FEBRUARY 2022
networkingplus.co.uk

NETWORKING+

Business broadband

Tips on searching for business broadband

Dominic Norton, Spitfire
p5

Cybersecurity attacks

History is not destined to repeat itself

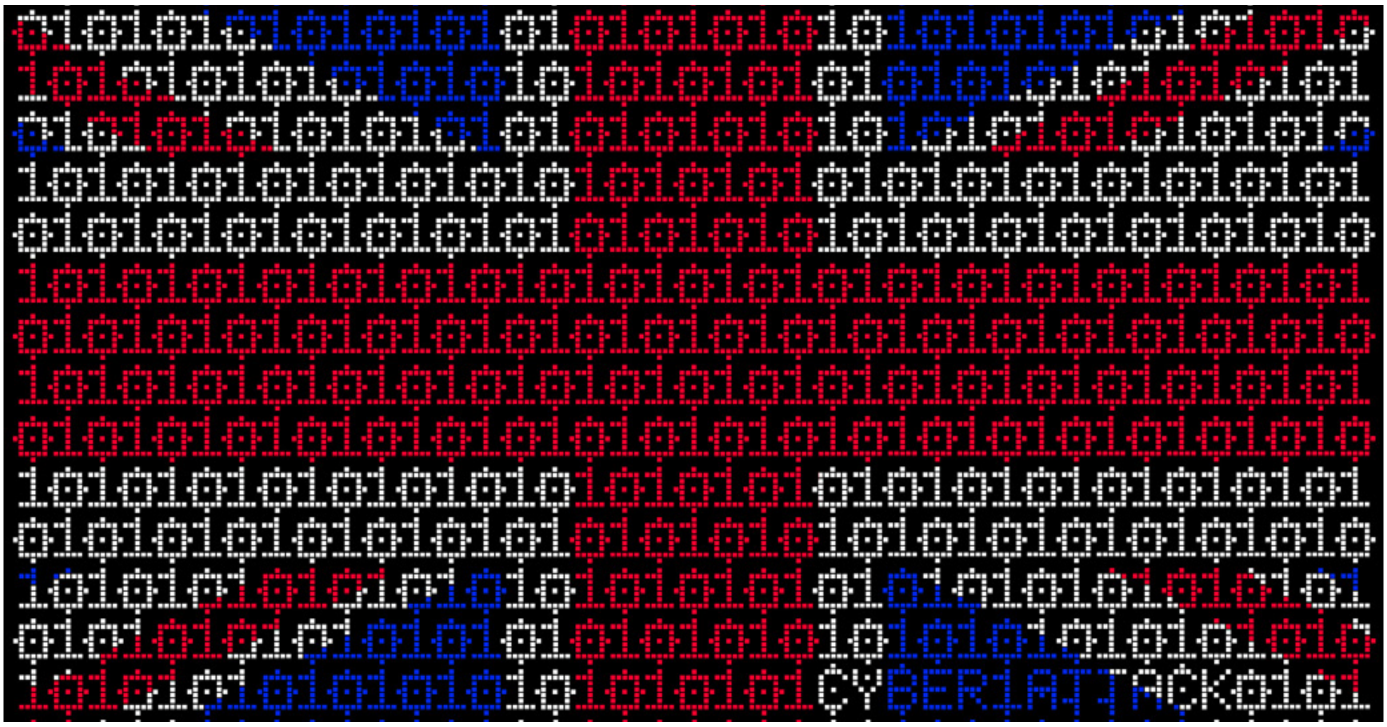
Galeal Zino, NetFoundry
p6

Questions and answers

A CEO's life away from the office

Rob Steele, Iplicit
p16

Record levels of investment for UK's cybersecurity sector



UK-registered cybersecurity companies raised north of £1bn in external investment across 84 deals last year, as foreign investors tapped into growth in capabilities such as network security and threat monitoring.

The record figures contained in the Department for Digital, Culture Media and Sport (DCMS) Annual Cyber Sector Report, which tracks the growth and performance of the UK's cyber security industry, reveals the sector contributed around £5.3bn to the UK economy in 2021. This marks a rise by a third on the previous year from £4 billion - the largest increase since the report began in 2018.

Employment across the industry rose by 13%, with more than 6,000 new jobs created, opening up new opportunities for people across the UK to join the sector and share its wealth. This brings the total number of people working in cyber in the UK to 52,700.

There were 1,838 active cyber security firms in the UK in 2021. More than half are based outside of London and the southeast, with cyber security showing growth in the northeast and East Midlands. The report highlights this move could be a result of remote working increasing regional opportunities.

Elsewhere, Bristol-based Immersive Labs raised £53.5m, while London-headquartered Tessia secured more than £52m in funding.

Nadine Dorries Secretary of State for Digital said that cybersecurity firms are major contributors "to the UK's incredible tech success story", which has laid the foundations for a bright future.

"Hundreds of British firms from Edinburgh to Bristol are developing and selling cutting-edge cyber tools around the world that make it safer for people to live and work online," she added. "We are investing in skills training and business initiatives to help the UK go from strength to strength as a global cyber power and open up the sector to people from all walks of life."

The UK attracted a number of foreign firms, with US-headquartered companies representing one in ten UK-based cyber companies, highlighting the importance of US-UK collaboration in this area to support the UK's economic growth.

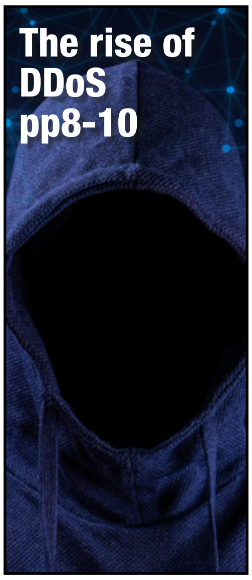
Vicky Brock chief executive officer (CEO) and co-founder of Vistalworks, said her company was originally founded in response to a Scottish government innovation challenge to find innovative technology solutions to online illicit trade.

"As we've grown, working closely with our government agency and cyber security stakeholders has remained incredibly important," she added. "The Cyber Runway Scale programme has enabled us to reach new public and private sector contacts, including contracts with banks and enforcement, and has helped us develop the skills and awareness we need to take our intelligence solutions to new markets and partners across the rest of the UK and beyond."

Lorna Armitage, co-founder at government-backed cybersecurity training firm Capslock, added: "The support of Plexal and government-funded programmes like Cyber Runway has enabled Capslock to accelerate our growth from a young startup in 2020 to the 'most innovative cyber security SME of 2021', as named by DCMS.

The government's National Cyber Strategy is supporting UK firms to grow through a number of schemes including the National Cyber Security Centre Startups and CyberFirst bursary schemes, the London Office for Rapid Cyber security Advancement and the Cyber Runway programme.

The DCMS has launched a number of skills initiatives including the Cyber Explorers youth programme and skills bootcamps. ■



The rise of DDoS
pp8-10

British Council: data breach leaks 10,000 student records

A security incident has exposed at least 10,000 records held by the British Council, a public sector organisation that provides English language courses worldwide.

The third-party breach was reported December 5, 2021 by researchers from security software development company Clario when they discovered an open and unprotected Microsoft Azure blob repository.

Clario said blob container was indexed by a public search engine, which researchers claim contained more than 144,000 of xml, json, and xls/xlsx files.

These datasets featured personal data belonging to students from around the world, including full names, email addresses, student IDs, enrolment dates and durations of study.

"It is unknown for how long this data was available online in public, with no authentication in place," Clario said in a blog post on its Mackeeper website.

Researchers contacted the British Council December 5 – then on December 23 the institution confirmed what it had found.

Clario researchers said that the repository "personal and login details of British Council students, potentially putting them and their personal information at risk".

They also advised any individual that may have been affected to change their passwords immediately and be on the lookout for suspicious-looking emails or links.

"Follow your instincts. Is that email or website looking dodgy?" the post added. "Did you suddenly get an advertisement, asking you to join a promo? Stay on high alert after a data breach to make sure you don't fall victim to a scam."

The British Council, founded by the UK government in 1934, promotes cultural relations and educational opportunities overseas. ■

Neos provides Oxon with public sector broadband

Neos Networks has secured a deal to provide it with full fibre gigabit broadband connections to over 200 public sector sites.

The 20-year agreement is backed by a £5m investment from the council and £2m from the Department for Digital, Culture, Media and Sport's GigaHubs project to boost full fibre provision in rural areas.

Neos will work with Openreach, Virgin Media Business and locally based Gigaclear to provide connections to sites including county council buildings, schools, libraries, GP surgeries, fire stations, leisure centres, community centres and museums.

The move builds on Oxfordshire's wider commitment to improve connectivity across the county through its Digital Infrastructure Programme. It has an ambition to equip community centres to become working hubs for services including health and social care support.

It is said to be the first majority council funded project aimed at improving the service offering available at community centres and village halls.

Additionally, the new infrastructure should enable the council to migrate to lower cost fast broadband connections for its office buildings.

"We are putting a lot of time and resource into ensuring that we are one of the best- connected counties in the UK," said councillor Glynis Phillips, Oxfordshire's cabinet member for corporate services. "This project strengthens our commitment to our digital infrastructure strategy and to improving local access to services, reducing the need to travel. We particularly look forward to finding ways to maximise the range of services that will be enabled in Oxfordshire's vibrant community centres and village halls where collaboration with parish, district, and the county council will be key alongside our colleagues in the NHS".

Neos plans to deliver the first phase of the programme by March 2022. ■

AtlasEdge acquires Leeds DC

Pan-European data centre provider AtlasEdge has expanded its operations in the north of England, with the acquisition of the largest purpose-built site in Leeds.

The data centre comprises the 11,000sq ft Cornelius House, bought for an undisclosed sum, from Hardy Fisher Services and adds to its existing sites in Manchester, Preston, Bradford and Huddersfield.

This acquisition is part of its plans to create "Europe's leading edge platform".

"We are very pleased to have acquired this data centre, adding an important location to our portfolio in the UK," said Giuliano Di Vitantonio, chief executive officer, AtlasEdge. "The Leeds site is uniquely positioned to act as a regional aggregation hub and will ensure AtlasEdge's distributed and highly connected footprint can support the next wave of growth in digital infrastructure for the surrounding area."

The Leeds data centre is connected to seven networks and AtlasEdge says it will develop the site into a regional aggregation hub. The firm stated that its "significant" existing connectivity would help it "accelerate time to market in the region".

"AtlasEdge is a very attractive buyer for us - their proposition is compelling and timely", added Jason Beresford, founding partner and chief executive, Sostratus Capital, owner of Hardy Fisher Services. "It is fantastic for AtlasEdge to be investing in Leeds and, as the first international data-centre player to do so, we believe they are ahead of the game. Being able to partner with AtlasEdge provides us and our customers the edge services we need to deliver our ambitious business outcomes. We are looking forward to further developing this relationship as both the market and demand continues to grow".

AtlasEdge was established through a joint investment by Liberty Global and DigitalBridge. It has more than 100 sites across Europe. ■

Manchester United hires Extreme to modernise network

Extreme Networks has agreed a multi-year partnership with Manchester United that will see the tech firm networking services and analytics to the Premier League giants.

In its capacity as the club's official Wi-Fi network solutions and official Wi-Fi analytics provider, Extreme will install a Wi-Fi 6 network at Old Trafford stadium, supporting the club's operations and providing fans with access to reliable connectivity.

Sporting arenas are technically challenging sites for mobile and wireless networks because of the bowl-like environment, the presence of tens of thousands of spectators and the fact that so many are uploading media rich content to social networks.

Wi-Fi 6, in conjunction with 5G, will help address some of these shortcomings by offering huge advances in speed and capacity. This enhanced reliability will allow United to rollout new services, such as mobile ticketing and digital signage. The move is part of the club's strategy to modernise Old Trafford following complaints of underinvestment in recent years.

Aside from the fan-facing applications, the club will also benefit from cloud-based real-time analytics that provide insights into what fans are doing in the stadium and identify potential issues such as bottlenecks or lengthy queues.

"Our collaboration with Extreme Networks is an important step in our drive to enhance and modernise the in-stadium fan experience at Old Trafford, opening up exciting opportunities for the club to deliver next-generation digital services to fans on matchdays and to visitors throughout the year," said Collette Roche, Manchester United chief operating officer. "With experience working with other iconic venues around the world, Extreme will help us keep our stadium up to date while preserving the character that makes it unique. Providing fast, reliable Wi-Fi to fans, underpinned by cutting-edge analytics to optimise performance, is a crucial part of that process."

United's IT department will also gain access to powerful monitoring tools that allow them to optimise the wireless network environments and identify any potential issues. ■

KP Snacks hit by ransomware attack, disrupting deliveries

KP Snacks, one of the biggest snack companies in the UK, was hit with a ransomware attack in late January, disrupting the deliveries of several popular crisps and nuts brands, including Skips, Nik Naks, Hula Hoops, and McCoy's crisps.

According to messages sent to local shops and published by industry news outlet Better Retailing, deliveries could face delays and cancellations up until the end of March at the earliest.

"At this stage we cannot safely process orders or dispatch goods," the letter from KP Snacks explains.

A company spokesperson has confirmed that KP discovered a ransomware attack on Friday January 28.

Max Locatelli, regional director western Europe at Infoblox, the IT automation and security company, said "with each year that passes", the ransomware threat to both individuals and businesses seems to grow. "As KP Snacks becomes the latest in a long list of high-profile companies falling victim, it's clear that no one is safe," he added. "It's never been more important for businesses to take steps to minimise the ransomware threat and protect their employees and their customers. However, in the majority of cases, this is much easier said than done."

Locatelli also said that when it comes to ransomware, "business leaders should zero" in on specific protection, "but also zoom out" to secure the entire IT stack. "Achieving full visibility and defending from the network edge will likely be a priority for security teams moving forward," added. "Leveraging DDI (DNS, DHCP and IPAM) sees DNS security come into play. DNS acting as the security control plane will give organisations the upper hand with a zero day strategy and enable them to protect their networks and their employees from the latest ransomware threats." ■

Max Locatelli, Infoblox

EDITORIAL:

Editor: Robert Shepherd
roberts@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Dominic Norton, Galeal Zino, Tim Wallen, Mattias Friström, Eva Abergel, Sean Newman, Richard Hummel, Chris Bujis, Andrew Fruish, Nick Sacke and Rob Steele

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

ISSN: 2052–7373

Vodafone Business and RingCentral introduce flexible cloud communications solutions

Vodafone Business has jointly developed Vodafone Business UC with RingCentral, a cloud communications platform that integrates the mobile network operator's 5G capabilities with its partner's technology.

The solution, to UK enterprises, combines internal messaging, video conferencing and cloud telephony in a single application that can be accessed from anywhere.

Vodafone Business products and services director Giorgio Migliarina stressed that as businesses adapt to a disruptive and changing environment, they "need to become more automated and agile" in the way they work.

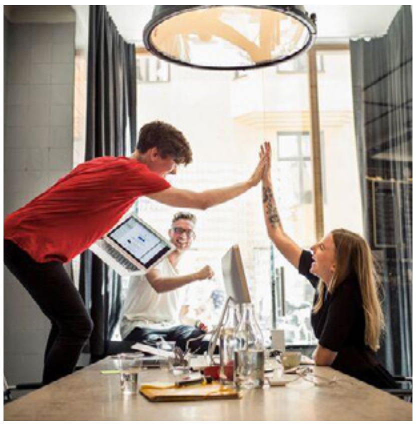
"Bringing technologies together that work in sync, connecting people, processes and information for faster decision making, will be critical," he added. "Vodafone is committed to supporting the digital journeys of companies big and small, so we're pleased to be working with RingCentral to support this move and help organisations become fit for the future."

Both companies described the platform as "highly secure and robust" and offers an expanded portfolio of next generation unified communication and collaboration capabilities including team messaging, HD video meetings and calling.

"Enterprises today have growing global communications needs to meet the ever-evolving demands of their mobile and distributed workforce—from servicing global customers to expanding their global talent pool," added Homayoun Razavi, chief business development officer, RingCentral.

All features can be run standalone or integrated with various business applications, including Microsoft 365, leading customer relationship management (CRM), enterprise resource planning (ERP) and helpdesk services – ensuring everything works in sync.

In addition, Vodafone Business UC with RingCentral includes real-time and historic analytics, extensive call management, and team collaboration and task management capabilities, which will be available to larger businesses. Vodafone Business plans to expand the platform to smaller businesses in the UK soon. ■



Motorola secures four-year Airwave extension with Home Office worth £1.56bn

Motorola Solutions will continue to provide mission-critical voice communications to public-safety services in the UK via the Airwave TETRA network through 2026, after the land mobile radio (LMR) vendor signed a four-year extension to the tune of £1.56bn with the Home Office.

Officials for both the government department and Motorola Solutions announced publicly the intention to continue use of the Airwave system through 2026, because the LTE-based Emergency Services Network (ESN) is not yet ready to replace Airwave. The annual financial terms of the four-year deal are similar to the previous three-year Airwave extension that expires at the end of 2022.

"We confirm that the Airwave network will continue to provide mission-critical services to the U.K. emergency services until the end of 2026, in accordance with the Home Office's requirements," Motorola said in a statement.

Initial UK government plans called for the Airwave TETRA system to be retired at the end of 2019, when the LTE-based ESN was supposed to be complete. However, ESN is still not operational, necessitating a first Airwave extension through 2022 and this second extension through 2026.

In addition to owning Airwave, Motorola provides the software and services for the much-delayed and over-budget ESN—a dual role that CMA has indicated will be examined as part of its investigation. ■

FROM THE COVER

Vertiv survey sees edge component of total compute growing by 29%

London, UK [February 24, 2022]
Significant, industry-wide investment in edge computing will change the profile of the data center ecosystem over the next four years, increasing the edge component of total compute by 29% over that time, from 21% of total compute to 27% in 2026. The magnitude of the industry's ongoing shift to the edge is among the notable findings from a new global survey of data center industry professionals from Vertiv (NYSE: VRT), a global provider of critical digital infrastructure and continuity solutions.

About a third (34%) of those surveyed are either planning or in the midst of significant edge deployments. A quarter already have deployed new, purpose-built edge sites, and 41% are operating legacy edge sites. All the activity at the edge is striking, but survey participants also anticipate a 150% increase in core sites and increased activity in the cloud. According to the survey, the percentage of IT resources deployed in the public cloud is expected to grow from 19% currently to 25% by 2026. The demand for computing resources is skyrocketing across today's networks.

"The next five years will reshape the data center landscape, shifting more and more computing to the edge while buttressing the enterprise facilities at the core of modern hybrid networks," said Martin Olsen, global vice president for edge strategy and transformation for Vertiv. "This survey makes clear the urgent demand for computing closer to the end user. The future of computing is about speed and latency, and the only way to meet the need is to build out the edge of the network."

The survey results arrive on the heels of the release late last year of Edge Archetypes 2.0: Deployment-Ready Edge Infrastructure Models. That report furthered Vertiv's research into the edge of the network and identified four edge infrastructure models that enable a more intelligent, semi-standardized approach to edge infrastructure deployment. The survey results are consistent with the premise of Edge Archetypes 2.0 – that massive growth at the edge necessitates a more standardized approach to edge architecture.

The survey also revealed the changing profile of the modern edge site. Twenty-nine percent of sites feature between 5 and 20 racks, and 13% have more than 20 racks. More racks mean more power, and the survey results reflect that: 28% say their sites require between 21 and 200 kW, and 14% report power demands in excess of 200 kW. The days of single racks tucked away in rudimentary IT closets are over.

Vertiv surveyed 156 industry professionals with insight into their company's edge computing plans. Complete survey results are available in the report, What's Your Edge?

Survey Highlights Infrastructure Transformation Occurring at the Edge of Network. Visit Vertiv.com for Edge Archetypes 2.0 Deployment-Ready Edge Infrastructure Models and a tool to identify the appropriate edge infrastructure model for your site.

BNP Paribas launches dedicated data centre team

BNP Paribas Real Estate (BNPPRE), the real estate unit of the French banking firm, has launched a new team focused on the leasing and land acquisitions of data centres across the UK. The company recently appointed Michael Umfreville to lead a new team focused on the leasing and land acquisitions of data centres across the country. "With data centre transactions heating up across the core locations, BNPPRE will provide support and advice to our clients, whether they are well established or entering the market for the first time," he said. The firm said its decision to create a dedicated team comes as specialist private institutions have begun to enter the data centre investment market, including REITs, institutional investors, sovereign wealth funds and infrastructure funds.

Boomi takes Solace

Boomi, the intelligent connectivity and automation firm, has partnered with event-driven-architecture (EDA) broker, Solace, to enable real-time data movement across the applications and cloud services used to run and differentiate its business. It will install Solace's PubSub+ Platform, an event streaming and management technology that streams master data from datacentres to enterprises in real-time. Boomi will use the technology to distribute product information on a real-time, event-driven basis instead of issuing daily batch updates. The platform is expected to improve the reliability, strength and agility of Boomi's infrastructure. "An event mesh built with PubSub+ Platform empowers Boomi to process data in real-time, leading to greater business and operational efficiencies," said Ed Macosky, head of product, Boomi. "One of the first ways we will leverage this new capability is by deploying a metering service."

Fabless semiconductor firm to slash DC energy usage and emissions

Fabless semiconductor company Cambridge GaN Devices (CGD) has launched a project called ICeData that could contribute to saving more than eight megatons - that's million metric tons - of CO2 emissions from data centres annually by 2030. The firm aims to develop and commercialise a highly efficient gallium nitride (GaN)-based integrated circuit (IC) for use in data centre server power supplies. "Exponential growth in demand for data storage and processing, accelerated by the Covid-19 pandemic where cloud-based connectivity became an essential tool for businesses around the world, is resulting in huge increases in data centre energy usage," said Giorgia Longobardi, chief executive officer and founder, CGD. Data centres had an electricity consumption rate of 400TWh in 2018, which is set to double by the end of this decade.

Swindon Borough Council and CityFibre bring full fibre connectivity to area

The rollout of a town-wide full fibre network in Swindon has taken a major leap forward thanks to a new £40m agreement between CityFibre and Swindon Borough Council. This new partnership will ensure the project can continue to go ahead smoothly and reach businesses as well as social housing sites and other homes in the area. "Swindon is set to become one of the best-connected towns in the country and this new agreement with Swindon Borough Council brings its full fibre future one significant step closer," said Neil Madle, CityFibre's city manager for Swindon. "We can't wait to connect communities across the town to our network so they can reap the benefits that come with future-proof digital connectivity."

Neil Madle, CityFibre

Pure shelves Herts data centre plans

Pure Data Centres has shelved plans to build a site in Borehamwood, Hertfordshire despite planning permission being granted last year by the local authority for the project at Panattoni Park. A spokesperson for Panattoni, which owns the land on Elstree Way, where

the data centre was to be built, said the deal with Pure did not complete. The plans, approved by Hertsmere Borough Council, would have seen a three-storey data centre constructed on the site of the former Sainsbury's frozen food depot. Instead, the site will be home to logistics facilities including the 159,000 square foot warehouse that has already been completed and is available for occupation.

New UK data transfer mechanisms

The UK Information Commissioner's Office (ICO) has published the final form of its much-anticipated new International Data Transfer Agreement (IDTA), along with a separate addendum to the EU SCCs (SCCs Addendum). The IDTA and the SCCs Addendum offer important alternative ways to ensure that UK personal data is adequately protected when exported from the UK. Assuming there are no objections from MPs, will go into effect on March 21, 2022. In addition, the UK has brought its approach to "restricted transfers" back into alignment with the EU. That means that some data importers that previously did not need to adopt the UK's form of SCCs must now meet this requirement.

Kids schooled on DDoS

The cybercrime unit of the UK National Crime Agency (NCA) is stepping up a programme designed to educate children about the ramifications of DDoS attacks. A post on its website explains how the initiative is informed by recent research that suggests kids as young as nine are guilty of launching DDoS attacks against their school networks, websites and other services. According to the report, the volume of such attacks has risen sharply during the pandemic, presumably causing disruption to online learning activities. The Cyber Choices campaign identifies potential offenders by tracking searches associated with cybercrime made by kids on school computers.

Word on the web...

Augmented reality becomes actual reality

By Sibongiseni Chili, product offer manager machine solutions, Schneider Electric

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

“There shouldn’t be a one-size-fits-all approach when it comes to business broadband

by Dominic Norton, sales director, Spitfire Network Services

If you use a broadband service at home, can you remember the selection process you went through before signing up? Probably not, but it might have been on the back of an offer from one of the well-known providers offering you amazing broadband speed, for example. However, when it comes to choosing broadband for your business, it’s a different kettle of fish entirely - selection criteria differ hugely between residential and commercial.

There are myriad choices these days - different speeds, varieties, providers and all promising to be the best with all the usual marketing and hype that comes from competing in such a congested market. The shift in broadband usage towards more real time applications has been especially highlighted by Covid’s impact on our working habits over the last 18 months or so.

Ultimately, the outcome or experience of using broadband in the home versus in the office can be wildly different. For example, a Zoom call to friends or family that ends up being patchy or juddery doesn’t signal the end of the world. That same Zoom call to an important client discussing new business could lose you money. Likewise, when watching TV at home via a streaming service it isn’t the end of the world if you suffer a patch of poor-quality service due to buffering. However, the same kind of delay with real time applications in a business setting can cause more significant disruption and impacts on productivity.

Speed

Fast speed does not necessarily equate to high performance. Don’t forget, business activities need high performance for applications to run smoothly and effectively especially for real time applications - high speeds don’t guarantee this required execution. It’s easy to get side-tracked by the marketing push on broadband speeds.

And so, what is the best speed for your business then? It largely depends on what your business does. Don’t forget, you actually need to consider two speeds, not one. There is upload speed and there is download speed. So, for example, the download speed will have an effect on receiving files such as documents, music or images and upload speed concerns itself with the sending of files. Try and work out the minimum speed you need and start from there - if you are just browsing the internet and using applications locally you probably don’t need particularly fast speeds.

Service

It’s probably true to say that most businesses these days rely on broadband connectivity for their business operations to run smoothly. Therefore, it is important to know how your chosen service provider’s ‘service’ actually performs on a day-to-day basis. This is where a Performance Service Level Agreement (SLA) is paramount - effectively detailing the performance parameters of the service. This will normally refer to the maximum levels of delay or packet loss that can be expected when data is being transmitted over the circuit. A performance SLA should also outline what the business can expect to receive if that provider’s performance service levels don’t meet the minimum stipulations. Think service credits. In fact, these SLAs should be addressed as a priority.

Support

Just as important as Speed and Service is what kind of support is on offer from your chosen provider. What you need to understand here is, how long is the fix time going to be if something goes wrong but also, how readily is the support service available (whether manual or automated). Again, sitting at home with poor or little service whilst you try and enjoy your favourite streaming service is annoying but not catastrophic. If your connection is failing whilst you are trying to host an important zoom meeting or trying to close a big sales deal, then the outcome to the business is more than just a minor inconvenience. This is where a support or service SLA is important. This may refer to a targeted uptime of the service and will include a contractual fix time from when a fault is reported. Again, you should expect to receive service credits if this is breached. So, make sure you know what the fix time would be if your connection does go down and have a plan B for working if the connection does drop out. And what happens if you do need to call the ‘help desk’? Is your support team on the other side of the world or are you dealing with dodgy voice automation and a series of infuriating voice menus?

As we have seen, choosing broadband for your business is a different affair to choosing what goes into your home. We can all deal with the relatively minor inconvenience of a Netflix movie going down, but your business can’t afford to be affected by too many failed connections or lousy quality video calls. And remember, it’s not all about speed. Don’t forget about service and support. ■

Cybersecurity attacks: history is not destined to keep repeating

By Galeal Zino, founder and CEO, NetFoundry

Here's a sad and simple 2022 prediction: cybersecurity breaches will be even more painful than the ones we suffered in 2021, even though attacks such as Log4j, the REvil ransomware attacks and Kaseya were among the most catastrophic in history.

The elephant in the room is that our networks are being attacked beneath the water line. Last year's high-profile attacks would not have been prevented by the zero trust solutions being sold by most vendors, because those solutions focus on the user-to-application connection – the activity above the surface – and the attacks target other connections.

Among the numerous doors beneath the 'water line' are:

- IoT and edge compute connections
- Application and web servers communicating with databases
- Data collector and agent (SIEM, APM, management) communication
- Remote administrators interfacing with servers and databases
- DevOps and CI/CD systems managing software and systems
- API and multicloud interactions

But it's not all doom and gloom. A more optimistic take is that 2022 could be the year when we start to turn the tide in the cybersecurity war by implementing zero trust design principles. We just need to apply these principles more thoroughly than we do now.

The problem for enterprises evaluating zero trust solutions is that it's difficult to tell the difference between the design principle, which is fundamentally sound, and the marketing label, which offers zero protection.

Most people by now understand the fundamental point of zero trust, which is to assume that any user, device or application trying to access any resource under your control is hostile until proved otherwise. That idea needs to be underpinned by a wider design principle:

1. Shift left to put secure networking into the heart of the development and delivery lifecycle.
2. Enable the makers (including development teams, NetOps, DevOps) to control secure networking, as code. Eliminate dependencies on telcos, clouds and infrastructure.
3. Enable makers to implement designs that shrink the attack surface and minimise the blast radius. Not just reduce but minimise – by design.
4. Eliminate the WAN architectures. Stop building inherently insecure WANs and then trying to bolt on security. Instead, build secure networking into the apps.

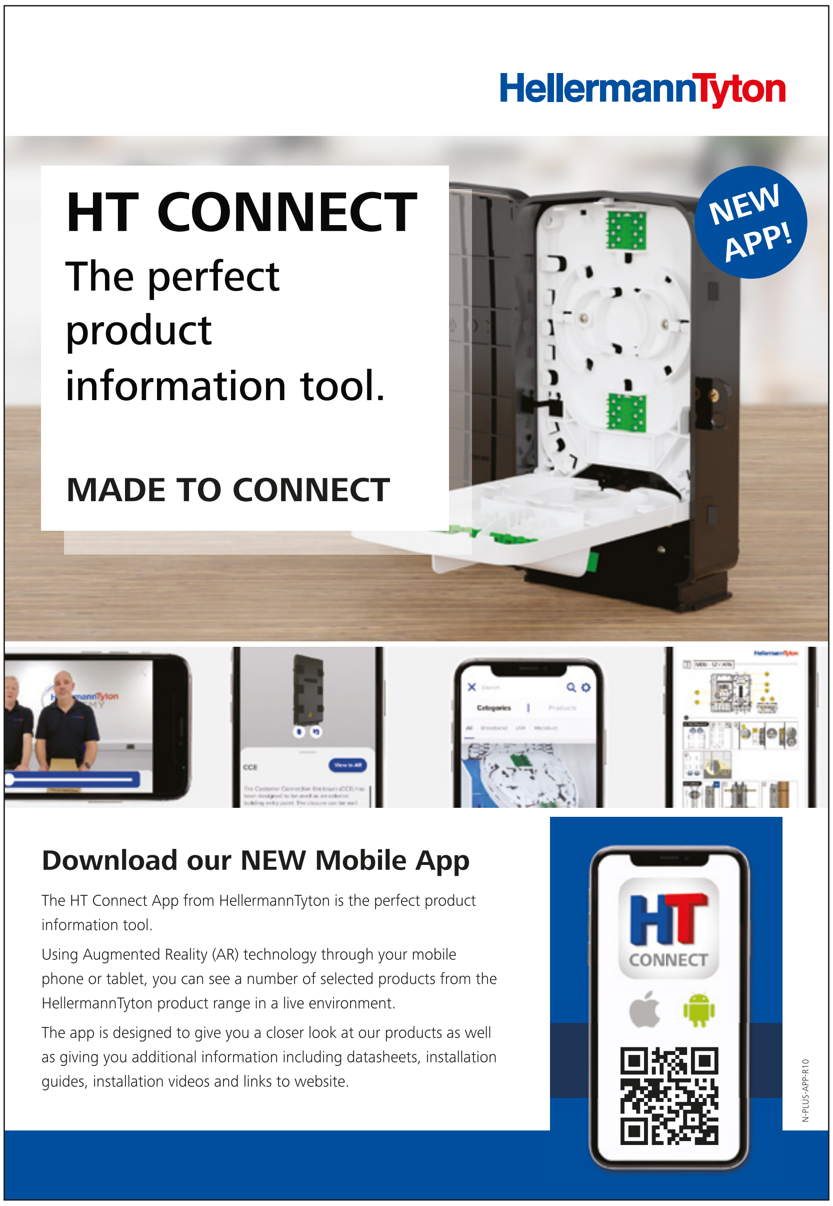
Here's how a zero trust networking design can function:

1. All network doors closed, by design. Not just the user to app door (above the water), but all the doors, including inbound firewall ports.
2. App sessions can't even knock on the doors until and unless they are strongly identified, authenticated and authorised. Hint: IP addresses are not sufficient.
3. If a session is authorised, then outbound-only connections are spun up, on demand. These are outbound from each side of the connection, brokered by a proxy, such that both sides can block all inbound sessions. The connection is ephemeral – spun back down after the session – so there is not a 'sitting duck' conduit for a future attack.
4. Those ephemeral connections are least privileged access and app specific - governed by centralised policies and orchestrated from the cloud, programmatically.

Zero trust networking principles and designs like the examples above can actually prevent attacks like Log4j and the ransomware attacks, and the same applies to IoT-centric solutions such as critical infrastructure, edge compute and connected vehicles. This is not to say we won't have Log4j like vulnerabilities – of course we will, that is the nature of software. But we make it so those vulnerabilities can't be exploited from the networks. So, the attack surface can be reduced from billions of Internet-connected nodes to maybe handfuls of people who have certain access to a particular server. At the same time, the blast radius has been minimised: the attack can't spread across the WAN if we've effectively eliminated the WAN.

I am confident that we will start to see these designs implemented in 2022. If we extend the range of the crystal ball to the following year, expect to see a Cambrian explosion of innovation. Makers freed from the limitations of today's inherently insecure WAN architectures and enabled to programmatically control secure networking, could unleash innovation in AI/ML, web3/blockchain and Industry 4.0. We won't see progress in any of those areas without truly secure networking.

If we're to get to that stage, the shift left in development is critical. Today enterprises depend on telcos, cloud providers and expensive hardware to provide security that – as recent history has shown time and again – doesn't fully protect them. Embedding secure networking as code at the heart of the development and delivery lifecycle will put in enterprises in control, and free them to focus on solving problems, serving customers and creating business innovation. ■



Why consolidation and automation should top your cybersecurity list

By Tim Wallen, regional director, UK&I, LogPoint

Traditionally, those charged with responsibility for cybersecurity, invest in best-in-class products from leading vendors to shore up the vulnerabilities that they perceive pose the greatest risk to their organisation. So, one year it could be a new EDR capability and the next year a sophisticated intrusion detection system for advanced attacks. And so, it goes on. It's got to stop and here's why.

With all the security products organisations have installed (up to 70 different solutions in some cases), and the dollars they have invested, they still remain vulnerable to cyberattack. And their security operations struggle to mount efficient an effective response. Colonial Pipeline, Brenntag, JBS Foods and AXA have all fallen victim to ransomware attacks in the past year even though they probably had a multitude of cybersecurity defences in place.

Buying more solutions doesn't solve the problem. With enabling technologies maturing, more organisations should look to move away from best-in-class point solutions to take up a more holistic and consolidated approach to cyber hygiene and cybersecurity.

Having the best cybersecurity solutions isn't necessarily right for everyone. Take those that fall into the mid-tier category for example, thousands of them lack cybersecurity resources and maturity. They constantly struggle to justify their cybersecurity budget and see significant improvements in efficiency or a reduction in organisational risk from their investments. And even though some can afford best-in-class tools they don't have the expertise to make the most of the highly sophisticated feature set.

Companies must seek a more consolidated and unified approach either from a single vendor or by leveraging open standards to achieve a unified result. A case in point is in SIEM and SOAR systems where SOC teams often struggle operating in different UIs and switching context between applications. It leads to user inefficiencies. But if you bring SIEM and SOAR capabilities into one system that collects, analyses and prioritises security incidents then analysts will be able to identify and resolve incidents faster and keep businesses safe.

And it's for all of the above reasons that we will see those mid-tier operations start to adopt unified and consolidated cybersecurity infrastructures.

Cybersecurity automation is the way forward

Artificial intelligence (AI) and Robotic Process Automation (RPA) will also play a fundamental role in making this consolidation happen. As technologies they have both matured to the benefit of many industries – and cybersecurity is no exception. So much so that it's fair to say that AI and automation will be the only way that organisations are able to keep pace with the constantly evolving threat landscape as well as the volume of attacks.

Death of the classic security playbook

The classic security playbooks in use today are static requiring a high level of sophistication and expertise. Not only hugely time consuming, they are also virtually impossible to keep current. The advent of AI-driven or even AI-augmented detection and response will see the static playbook surpassed by a dynamic, real-time playbook that relates to current incident.

Based on analysis of incident case data, telemetry readings, historical cases and how they were resolved, threat intelligence from the Internet, and other sources, the AI-driven system will create the best playbook on the spot. You can execute the response automatically or require the analyst to OK the playbook actions. It's that simple.

Data driven cybersecurity

Central to maintaining a robust security posture is the need for accurate data. It's essential to mount an effective defence from both internal and external threats. That's in addition to a platform that pulls all the cybersecurity data together, verifies it, gives it context, simplifies it, and prioritises it based on urgency, past experience, potential damage, damage already incurred and many other factors. They need data to orchestrate the different tools in their cybersecurity infrastructure, so each tool plays its part fully and to maximum advantage. They need data to automate. If you can't trust your data, you can't automate the processes that use it.

Furthermore, new instrumentation capabilities mean CISOs can measure every component of performance and effectiveness of their overall security infrastructure. Having easy to digest cybersecurity metrics and data ensures CISOs can engage in performance and funding conversations that are much more productive.

Cyberattacks across the globe are increasing in sophistication and speed, threatening businesses of all sizes and industries. At the same time, security teams are confronted with a global shortage of cyber talent, minimising resources. As a result, SOCs struggle to quickly detect, investigate and respond to threats.

Taking a holistic approach to cybersecurity characterised by AI-driven consolidation of capabilities, unified instrumentation and automation will minimise the time it takes for security teams to detect, orchestrate and respond to cyber incidents. It will also help simplify and make their security operations more effective than they ever thought possible. ■

The rise of DDoS

DDoS is not a new form of cybercrime, but it's hammering networks harder than ever. Robert Shepherd asks why this is and how it can be contained

It's difficult to close an edition of this magazine without reporting that a cyberattack recently took place somewhere. Just leaf through the first few pages of this one and you'll see what I mean.

Of course, depending on who you speak to, there are several reasons why cyberattacks, cybercrime, hacking – whichever term you so choose – are becoming more prominent.

However, one form of cybercrime that, perhaps, hasn't featured as prominently or frequently as some of its more high-profile cousins is a distributed denial-of-service (DDoS), a subclass of denial of service (DoS) attacks is, quite simply, a cyberattack in which the bad actor seeks to make a machine or network resource unavailable to its users by disrupting – services of a host connected to a network.

One of the reasons for that is they are not new, having been around for at least 10 years and they happen all the time. So, to report one happening – unless it was unique – wouldn't add much value.

However, since 2021, the rate in which DDoS attacks are launched has soared to heights never seen before.

Richard Hummel, ASERT threat intelligence lead at Netscout says cyberattack activity has been increasing and evolving in recent years and "a catalyst for this is the mass adoption of hybrid and remote work models" due to the continued Covid-19 lockdown

> "As more and more businesses are dependent on a working network unfortunately hackers see new ways of threatening resource owners and thereby ask for ransom money to unlock systems or stop attacks"
>
> *Mattias Fridström, Arelion*

restrictions and work-from-home orders over the past 18 months. “To cause maximum disruption at a time of great upheaval around the world, cybercriminals have launched DDoS attacks to intentionally overwhelm online services to the point of crashing,” he adds, “And, in our interconnected world, many of these attacks have had a domino effect on global supply chains, making them a dangerous threat to worldwide industries.”Netscout’s recently published Threat Intelligence Report reveals 5.4 million DDoS attacks were reported in the first half of 2021, representing an 11% per increase from the year before – which was already a record-breaking year for DDoS attacks. When it comes to the reasons behind the surge in DDoS attacks, Hummel argues that it can be attributed to several factors. “Firstly, during lockdown restrictions, online infrastructure became more important than ever for keeping dispersed workforces connected and businesses in operation,” he adds. “A surge in online activity is an opportunity to launch damaging attacks. Taking full advantage, cybercriminals adapted their attack methods and targets.”

This can be seen with the internet publishing and broadcasting sector, inhabited by services such as Zoom, Microsoft Teams and other video conferencing applications, which have been crucial to continuing business meetings, online learning, and connecting with loved ones. For the first time, this sector became one of the top ten most attacked industries in 2020 and was among the top five most targeted industries in the first half of 2021.

Another factor is that many internet users are no longer safeguarded against cyberattacks by enterprise-grade security systems when working remotely. Threat actors have exploited these vulnerabilities, which has led to more incidents like the Lazarus Bear Armada DDoS extortion attacks, which targeted Virtual Private Network (VPN) concentrators. What’s more, attackers are generally now capable of disrupting an entire business instead of the 10-20 per cent of the workforce which was the focus prior to the introduction of the lockdown measures and work-from-home orders.

Mattias Fridström, chief evangelist at Arelion (formerly Telia Carrier) also concurs. “As more and more businesses are dependent on a working network unfortunately hackers see new ways of threatening resource owners and thereby ask for ransom money to unlock systems or stop attacks,” he says “With an increased value of the online business the grade of sophistication is following along.”

“In our experience it is not becoming more sophisticated particularly, but there are more tools and they are easier to access”

Chris Buijs, NS1

Sean Newman, vice president, product management, Corero Network Security, explains how the increased sophistication is linked to the fact that “the cyber landscape as a whole has long since moved from hacking with mischievous and publicity intent”, to organised cybercrime focused on financial gain.

“And DDoS is no exception, with attack motives shifting from traditional religious, political or moral grounds to being more financially motivated, with DDoS for ransom experiencing a significant rise over recent years,” he says. “By its very nature, DDoS is open loop – attacks are launched from across the internet, with no return traffic to the perpetrator, as is the case with data breach attacks. This means the original attack source is extremely difficult, or impossible, to trace in most cases, making DDoS an ideal tool for someone with criminal intent. The promise of healthy ransom demand payments, with relative impunity, has helped to drive the increase in attack numbers to another level.”

However, there are some who argue it isn’t necessarily so that the bad actors have become more sophisticated. One of those is Chris Buijs EMEA field chief technology officer and senior product manager for emerging products at NS1 DDoS attackers are usually motivated by creating the biggest disruption and reputational damage they can or for extrapolating data. “In our experience it is not becoming more sophisticated particularly, but there are more tools and they are easier to access,” he adds. “The move to the cloud and proliferation of digital devices also allows attacks to be launched from multiple vectors to amplify the magnitude, which makes them more effective.”

Newman adds that with a financial gain at stake, attackers are motivated to increase their efforts to ensure their attacks can successfully impact their victims, which is driving the increasing sophistication. “Cybercriminals understand that their potential victims are increasingly deploying some level of DDoS protection, so they must work harder to develop new attack vectors which can bypass these defences, which is driving up the levels of sophistication employed,” he says.

What’s also alarming – worse in some ways – is the morphing demographic of the people behind these attacks.

Indeed, the cybercrime unit of the UK National Crime Agency (NCA) is ramping up a programme designed to educate children – yes, children – about the ramifications of DDoS attacks. That’s because kids as young as nine have been caught launching these attacks against their school networks. Not only is DDoS becoming more common, the perpetrators are getting younger.

So, we know DDoS attacks are becoming more common and sophisticated, as well as the fact they are being orchestrated by children of junior school age. However, where does this strain of cybercrime rank in terms of seriousness and potential severity?

Fridström says “it’s very difficult to compare” and is very much up to the attack itself. “A large overflow attack can bring down complete networks for hours if you are not protected enough,” he continues. “Our research from last year showed that the impact of these DDoS attacks can be dramatic for some businesses, with 11% of respondents saying that such an attack has posed a threat so serious that it could have undermined business continuity. A further 40% said that such an attack had a major impact, resulting in significant disruption and loss of business revenues.”

Enterprises have a enough security concerns to deal with, but how does DDoS rank alongside its evil cousins?

Eva Abergel, security product lead at Radware, says that compared to other cyberattacks, such as malware, for example, the main threat associated with DDoS attacks is the loss of service availability, which occurs when a network slows down or is completely taken down. “While DDoS attacks don’t expose sensitive information, they can impact the SLAs between an organisation and its users as well as block legitimate users from accessing applications and services,” Abergel adds. “This can impact customer satisfaction, damage brand reputation, increase customer churn and lead to revenue loss. In addition, DDoS attacks are sometimes used as a smoke screen to hide other more targeted attacks. So, while an organisation is dealing with a DDoS attack or a ransom DDoS threat, the hackers are, in parallel, launching other invasive attacks to gain access to the company’s network, applications and sensitive data.”

Newman agrees that the seriousness of a DDoS attack depends on its target. “Used in isolation, they do not result in data breaches, which may lead some to believe they are not that serious compared to other cyberattacks,” he adds. “However, DDoS attacks cause significant disruption to Internet access and the applications, services, users, and customers that depend on it. DDoS reduces business continuity and can seriously impact revenues, reputation, customer satisfaction and loyalty, as well as employee productivity.”

Nevertheless, enterprises need to have safeguards in place to mitigate any DDoS attacks should one or more be visited. So, what are they?

“Companies can build resiliency, particularly to volumetric attacks by ensuring they have a more distributed, always-on, redundant DNS in place,” says Bujis. “It allows a second DNS network using separate infrastructure to be deployed in the event of an attack compromising the primary DNS and allows traffic control to shift bad traffic away when needed. Network managers can also leverage AnyCast protocols. These enable DNS requests to be diverted to an available server to guard against the impact of an attack on resources, or due to cloud resource overload or CDN outages, of which there were many in 2021. They can also use their own real-time data about network conditions to dynamically load balance between resources in the event of traffic spikes due to a DDoS attack.”

“At the high-end, implement a multi CDN (content delivery network) or cloud-based solution”

Andrew Fruish, Nene Cyber Security

“To cause maximum disruption at a time of great upheaval around the world, cybercriminals have launched DDoS attacks to intentionally overwhelm online services to the point of crashing”

Richard Hummel, Netscout

As far as Andrew Fruish, director of Nene Cyber Security is concerned, a basic defence that can be deployed is to make a plan, keep your systems patched, use a web application firewall WAF, monitor your network and look for the signs “[It’s key to] use large bandwidth capacity and server capacity to absorb and mitigate attacks,” he adds. “At the high-end, implement a multi CDN (content delivery network) or cloud-based solution.“

Abergel argues that basic tools simply block volumetric attacks and that whenever the traffic to a certain server exceeds a predefined threshold, traffic is totally blocked so that nothing can access the destination. “This method will protect a server from going down but only when basic attack tools are used and at the expense of service availability to legitimate users,”

High-end safeguards protect assets using a different approach. They use behavioral algorithms that can differentiate between legitimate and malicious traffic. When using algorithms,

“While DDoS attacks don’t expose sensitive information, they can impact the SLAs between an organisation and its users as well as block legitimate users from accessing applications and services”

Eva Abergel, Radware

there is no need to wait for an attack to reach a certain volume before stopping it.

The behavioral capabilities analyse the traffic instantly and put the right signatures in place, so that all malicious traffic is blocked, while legitimate users still have access to the server. This method ensures constant service availability, a better user experience and revenue protection. Additionally, there are sophisticated attacks that only high-end safeguards can detect and mitigate. These include burst attacks, encrypted attacks, IoT botnets and DNS attacks.

Does that mean that, in some cases, that a ‘successful’ DDoS attack on an enterprise could be linked to complacency on the part of the network manager or senior members of the security team?

“The less user error your organisation demonstrates, the safer you’ll be, even if there’s an attack but your organisation should also implement network resilience strategies such as more bandwidth or a cloud-based solution and have a response plan should attack occur,” Fruish adds. “In the majority of cases it’s possible to defend against DDoS attacks by implementing the industry’s best current practices.”

Nevertheless, according to a number of security experts, companies really do need to get their own house in order. After all, to use a social analogy, if you leave your front door open, there’s more chance of you being burgled.

“There are still far too many unprotected servers and applications in the network that do not require an advanced DDoS attack to be taken down,” says Fridström. “With proper protection hackers would have to become much more intelligent than currently many of them are.”

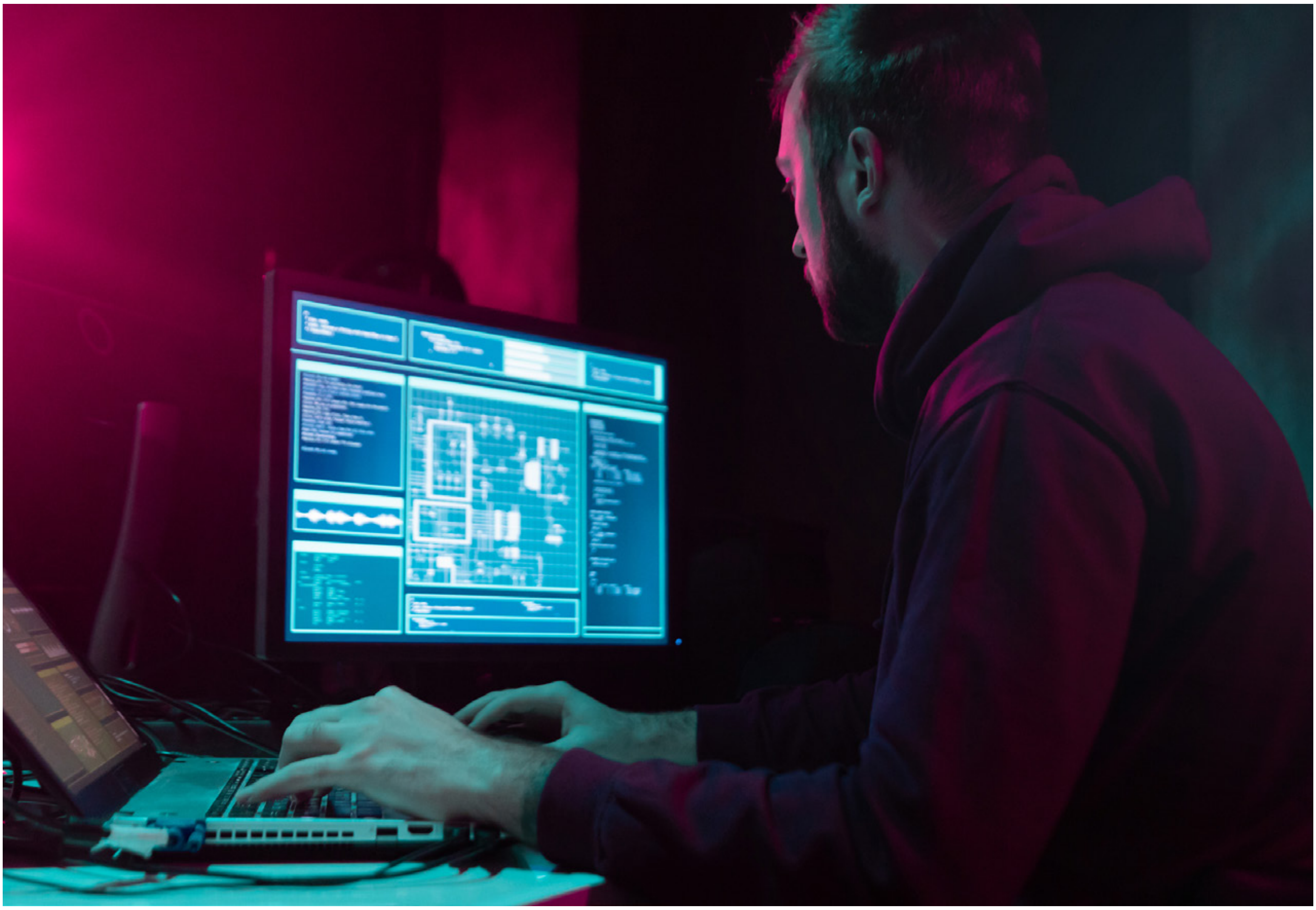
Putting security measures in place to combat DDoS is an obvious requirement if you value your business, but as the perpetrators and techniques become more sophisticated, the landscape will constantly evolve. To that end, Hummel says organisations need to invest in a powerful and effective DDoS mitigation system. “This will defend their public-facing online infrastructure before an attack occurs, providing them with peace of mind if and when they become the target of a DDoS attack,” he adds. “Generally, damage from an attack is minimal to organisations that proactively secure their systems with strong DDoS protection.”

Hummel adds that businesses should also test their DDoS defence systems on a semi-regular basis. That’s because it ensures that any upgrades made to the online systems are incorporated into the overall DDoS defence plan. “As such, the entirety of an organisation’s online infrastructure will be well protected. When defending VPN concentrators, organisations should consider implementing an on-premises ‘stateless’ solution,” he continues. “The use of stateless packet processing technology, in addition to utilising an advanced defence solution at the perimeter of the network, will detect DDoS attacks instantly. This rapid detection means that the business will be notified of the attacks before any serious damage is done. While many countries’ social distancing measures have now ended, the vulnerabilities exposed from pandemic-driven remote working still remain.”

“By its very nature, DDoS is open loop – attacks are launched from across the internet, with no return traffic to the perpetrator, as is the case with data breach attacks”

Sean Newman, Corero Network Security

So, there you have it – DDoS isn’t going anywhere other than fast in the wrong direction as far as businesses are concerned. However, implementing robust preventive measures, organisations will be in a much better position to defend themselves. ■



A tale of north and south of the border

Barnsley Council completes its SAP-to-Azure migration, while The Highland Council implements a Wi-Fi solution for tourists, visitors and citizens

Absoft completes collaborative SAP-to-Azure Migration with Barnsley Metropolitan Borough Council

When Barnsley Council first opened a bid in order to migrate its SAP landscape to the cloud, the tenders received did not offer an economically viable outcome. However, a non-negotiable deadline (the sale of its current premises and an outdated on-premise functionality) meant that a solution was required sooner rather than later.

The council initially issued a brief for a one-provider solution to migrate and run its SAP environment in the cloud. The tender requested that the critical run aspect of the scope covered the multi-year provision of the cloud infrastructure on which to run SAP, plus associated technical managed services to manage and maintain the SAP landscape.

Independent SAP consultancy and Microsoft Gold Partner, Absoft had anticipated the likely problems the Council would face with tender responses early on. Following the completion of the procurement process, Absoft reached out to the Council and, building upon a relationship established during the tender process, suggested various solutions.

The solution co-development

The key components of the original brief lay at the heart of the problem and therefore at the heart of a solution that Absoft proposed. Any solution had to address three facets: the provider landscape; the migration to the cloud project and subsequent running of the cloud-based SAP systems. Additionally, affordability was critical.

Provider landscape

Absoft became increasingly aware of the capabilities of the council's in-house technical team and after further discussions, the option crystallised for the in-house technical team to assume responsibility for running the SAP landscape.

Absoft confirmed the feasibility of this and suggested that, depending on the selected infrastructure provider, Absoft – or another specialist partner - could provide support where additional help may be required. This joint decision to utilise the internal team significantly reduced the project scope and required budget.

The successful bid

Absoft's success in this bid was attributed to a number of key differentiators, including a successful track record in migrating 17 SAP landscapes into the cloud – including cloud migrations from local authority "on premise" to the Azure Cloud. Furthermore, the combined Azure and SAP expertise and capabilities of Absoft meant no third party was required and the bid was affordable and well within the nominated budget.

The migration Project

Upon agreement of contract, the work commenced in March 2021. Shortly after this date, the initial project timeline was significantly reduced to a period of just 12 weeks.

A technically-challenging project, operating systems were different between the Production, Test and Development instances, with a total 128 interfaces to test. Risks represented by out-of-date business data and confusion generated from orphaned solutions was significant.

Furthermore, the deadline of twelve weeks was hugely aggressive – but immutable. Many late nights, early mornings and hours over multiple weekends were required to get the job done.

The result

The migration work was achieved within an unprecedented timeframe. The SAP and Azure skillsets of Absoft and its expertise in the UK public sector were instrumental in making sure this project was successfully completed, on-time, and within budget.

Based on Absoft's expert understanding of the available technology options, the company was able to provide a cost-effective approach to the migration, taking into account maintenance dates, software versions, and future-proofing the environment.

Through the enablement of the internal team, Absoft saved the client circa £125,000 in ongoing operational support fees for a Council under significant budgetary pressure. ■

> "I just wanted to take the time to say a huge thank you from the Barnsley SAP Team – you well and truly deserve it. We are in awe of the Absoft team – having an appreciation of the task that you've achieved, it's still hard to believe how easy you made the transition look. "You have done an exceptional job in keeping us all on the straight and narrow; we work with so many IT suppliers and I must say that working with Absoft has been an absolute pleasure"
>
> *Sara Hydon, head of ICT, Barnsley Metropolitan Borough Council*

Inverness Wi-Fi pilot

Inverness is the largest city in the Scottish Highlands and its city centre now has free public Wi-Fi following a collaboration between The Highland Council, Purple and Rapier Systems. The Highland Council wanted to implement a Wi-Fi solution that would allow them to identify who visits the city and gain a way of effectively communicating with visitors. Through the installation of Purple and Ruckus equipment by Rapier Systems, the council can now access a wealth of visitor analytics, all via a simplistic portal dashboard whilst visitors enjoy free, fast Wi-Fi whilst shopping, browsing, working and dining in popular zones of the city centre.

The challenge

The Highland Council recognised that city centre visitors now expect Wi-Fi as standard and that a lot of metropolises around the world are starting to offer free connectivity. People want to be able to browse the web, access social media and engage with online content whenever and wherever they may be. Therefore, to meet the demands of their consumers the council sought a free, secure, connectivity solution that shoppers, visitors, residents and local business owners could access.

Gaining a detailed understanding of who actually visits Inverness, including visitor names, ages, gender and where they've travelled from was also important to the council. Having limited visibility of their visitors prohibited them from making effective, strategic changes to the city's facilities, events and promotions according to their core visitor demographic. It also stopped them from delivering relevant, targeted communications to specific customer segments and individuals.

Finally, growing profits for city centre businesses is important to the council, so they sought a solution that would allow them to identify how long people dwell in the centre for and how often they visit. This information would help them to work out what can actually improve dwell time and ultimately lead to people spending more money whilst in the city centre.

Discussions and installation

Rapier Systems reached out to The Highland Council to see if they were interested in making the city smarter by introducing Purple's Wi-Fi and analytics solution. The firm was invited to host a presentation and detailed demonstration of the Purple product to showcase how the solution could potentially benefit the council, their visitors and local businesses.

The demonstration from Rapier Systems left the customer very impressed the council agreed to the tender for a preliminary trial, which would see Purple's Wi-Fi and analytics platform plus Ruckus hardware go live in key zones across the city centre for a one year period.

Rapier Systems installed the package at the city's famous Victorian Market plus other popular streets in the centre, including Union Street, Church Street, Falcon Street, Queensgate and Academy Street. The solution officially went live in December 2016, just in time for the busy festive period.

Lucrative outcomes

The city's Wi-Fi network has received almost 17,000 users in just six months, with the majority of individuals using the network for 1 hour or more. Thanks to Purple's platforms, the council can identify exactly where visitors are from, with the top three visitor locations including Inverness, Aberdeen and Glasgow. Through identifying where people are from they can ensure that any events hosted in Inverness don't clash with other happenings in cities where visitors often travel from.

When the visitor reports are exported the council can clearly identify who are their most frequent visitors, what the most popular age group is, when peoples' first and last visit was, amongst many other stats which can be used for both marketing purposes and to help plan for the city's future. Data about visitors will also be shared with stakeholders, groups, business to make more informed decisions which may have an effect on the city and surrounding areas.

There seems to be a clear balance between the number of males and females that visit the city centre, with 57% opting to login to the Wi-Fi network via a short form. Whenever a user accesses the network they are prompted to 'like' the official Highland Council Facebook and thanks to this feature the page has received a significant increase in engagement and 'likes'.

People, places, presence

Rapier Systems has recently activated presence analytics for Inverness city centre, which enables the council to gain an even deeper understanding of their visitors. With presence reports, the council can identify exactly how long people stay for on average, the split between repeat and new visitors and the most popular time of day for people to visit. This information is extremely useful for the council, especially when events are being hosted at the city. The team will be able to easily measure how successful an event was by seeing if there was an increase in the number of visitors at a certain time and an increase in dwell. They can also cross reference this information with local businesses to see if it increased sales and visitor numbers.

The Highland Council has been impressed with the solution delivered by Rapier Systems, Ruckus and Purple and has recently agreed to roll out phase three of its city centre Wi-Fi Project after a very impressive pilot. Phase four aims to take the project model out to towns throughout the highlands using the existing model created from the pilot and main roll out. This project is seen as an important part of the digital upscaling of the Highlands Region. ■

Using a blend of networks to achieve production scale in IoT developments

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

Why are there different IoT networks and protocols?

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

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

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

Which network type or protocol to use?

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

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

Use cases

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

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

Blended connectivity

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

Futureproof

Longevity is crucial for IoT success, and it is clear that LoRaWAN is on a growth trajectory that will provide this. And the eventual maturity of 5G will also become another option for IoT projects, with the capability to efficiently connect millions of sensors.

With a blended model of different protocols covering each estate, it's important to use a single platform to bring it all together to be analysed in one place. By working with a partner offering all types of IoT connectivity in a blended solution, projects can be rolled out in the confidence that each protocol is supported, maximising both functionality and practicality. ■

The challenges, opportunities and essentials of data centre management

By Diego Chisena, software and monitoring hardware offering manager, Vertiv

Data centre construction is booming in Europe with new project builds increasing by 60% from 2021–2022, compared with the 2019–2020 period. Additionally, the European data centre market is expecting revenue growth of up to 46% over the next three years.

Large investments in today's data centres and the adoption of edge computing sites mean operators are faced with managing more distributed environments.

To leverage the introduction of advanced toolkits, operators must aggregate and manage monitoring software holistically. This is in addition to the pressure operators are under to increase data centre availability, utilisation and uninterruptible service in the face of outages.

Here, operators are turning to date centre management tools to improve operational efficiency and the health of their equipment.

Adopting today's data centre management software solutions allows operators to collect the data required to run critical infrastructure effectively and efficiently.

Providing a comprehensive view of a system's operational performance, a data centre management tool gives real-time monitoring and insight to help govern capacity, maintain high availability readiness and reduce risk.

By alerting operators to critical problems caused by mechanical or human error, infrastructure monitoring deployment means issues can be identified proactively, resulting in reducing or eliminating outages.

When investigating the solutions afforded by monitoring technology, it's important to examine the situations causing the pain points in managing your data centre or critical facility.

Against this backdrop, here are the key functions to consider when implementing a data centre management solution.

Data centre operators need to know the equipment availability and capacity in their facility to identify changes for peak performance. The best tools allow operators to easily place and monitor specific devices based on system intelligence. By doing so, you can tailor the processes bespoke to your organisation's needs.

Furthermore, the introduction of data centre management software can overcome the most persistent obstacles to the remote management of distributed and hybrid architectures. Built on a common architecture, with open standards, platforms and APIs, it enables fast and scalable deployments of critical infrastructure equipment from the enterprise to edge to match data centre growth.

Modern data centre management solutions support a secure remote working experience, allowing systems data to be accessed and controlled quickly and seamlessly. In turn, this helps operators meet worker demands for today's advanced engineering and design requirements and high-resolution streaming applications.

As infrastructure becomes more complex, remote visibility and access to critical devices provide the means for operators to ensure users have uninterrupted access to perform their daily activities.

Data centre monitoring tools enable better power system management. Having a comprehensive view of the data centre power system, from incoming utility power to rack power distribution, creates a dynamic one-line diagram, helping to ensure business continuity.

Operators can forecast power consumption based on current and historical data. Using data centre capacity objectives, you can plan deployments and map out your IT equipment's dependency on the power system, aiding in risk assessment.

Another element of data centre management is the provision of advanced thermal management capabilities, evenly distributing available cooling capacity between IT devices and the facility. Its tools enable monitoring, reporting, and alarm management for the entire mechanical chain.

Offering around-the-clock access to your data centre through your mobile device, data centre management gives real-time visibility into your critical facility. This allows you to maximise capacity, prevent unplanned downtime, and monitor overall efficiency performance.

With budget and performance in mind, it's important to select scalable monitoring tools that allow implementation to be timed and aligned with your changing business needs.

Operators should decide what functionality is most essential by beginning with the main issues negatively impacting operations. As priorities change, so too should your infrastructure and monitoring plan.

While data centre management software can help organisations realise the advantages of increased utilisation, optimised efficiency and greater staff productivity, it's not a magic bullet.

When planning monitoring initiatives, you must consider what technological and infrastructure software innovations will come next. For example, a strictly reactive approach to managing issues within your critical facilities may not be enough for your organisation to achieve its availability and sustainability goals.

You may need a more predictive approach that's built on the foundation of infrastructure monitoring solutions, such as data centre management as a service (DMaaS). This is about tapping into a larger data lake, integrating operational data, and analysing at scale to inform all aspects of critical facility management.

With expanding use of data-intensive technologies and IT platforms in more locations outside the traditional confines, data centre management platforms must evolve to meet these challenges and accommodate next-generation applications.

Operators utilising a holistic approach via data centre monitoring solutions are better equipped to proactively identify issues before they escalate.

By using these tools, operators can ensure the right information goes to the right people at the right time, resulting in better management decisions, reducing day-to-day costs and increasing efficiency.

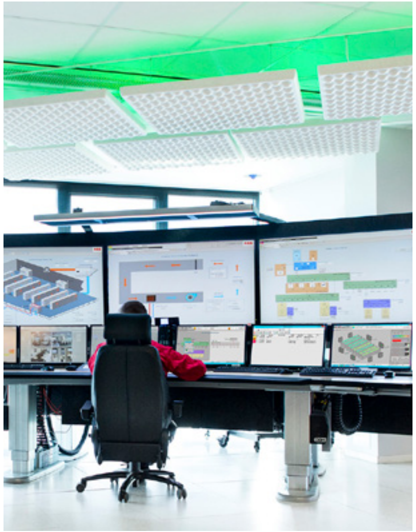
PRODUCTS

Lansweeper is a cross-platform IT asset discovery solution that finds and gathers information on all assets, listing hardware specs, installed software, user details, and more, the company says. This kind of end-to-end visibility can help you save valuable time and resources within your IT organisation. The main selling point of Lansweeper is its ability to discover any asset in your data centres without installing any software on them. This DCIM solution is a strict IT inventory management tool. That means you don't get a comprehensive CMDB that integrates with data centre management or IP address management. If you consider Lansweeper, remember to plan for these external capabilities. *lansweeper.com*

ABB says one can control, monitor and optimise for your mission critical infrastructure, with mechanical (BMS), electrical (EPMS) and DCIM capabilities in a single, industrial solution.

ABB Ability Data Center Automation is ABB's industrial solution for on-premise and hybrid cloud environments. At a base level, it is an integration and automation platform to enable transparency and interoperability for continuous optimization and high availability.

Its open, integratable platform and controls allow data exchange and automation among systems, equipment, components and applications so you can integrate data centre tool sets faster, including uploading assets into tracking tools. The service also integrates data from IT, power, cooling and building systems. Imagine: No more manual data entry to calculate utilisation metrics and other KPIs. *new.abb.com*



RackTables is a data centre and server room asset management solution designed to help the user document hardware assets, network addresses, space in racks, network configurations, and more. This open-source solution provides basic DCIM features you'd expect, such as documenting NAT rules, storing your load balancing configurations, attaching files to system objects, and assigning permissions for users—all without exhausting your budget. However, like most open source DCIM solutions you'll find on this page, RackTables requires you to keep everything updated manually, minimising your ability to streamline IT processes. While the solution provides basic rack layouts, you'll want a different solution if you need your DCIM solution to manage room layouts. *racktables.org*

Sunbird's second-generation DCIM software is described as "the easiest, fastest, and most complete DCIM solution and fulfills all the promises left unkept by first-generation counterparts".

The company reckons modern data centre professionals choose Sunbird as the best DCIM software to maintain uptime, increase the efficiency of capacity utilization, and improve the productivity of people.

Sunbird also claims to be "the pioneer of second-generation DCIM, with key pillars" including:

ease of use (elegant web-based GUI that requires fewer clicks and mouse movement and is intuitive to use), zero-configuration analytics (pre-built dashboards, charts, reports, and visual analytics come out of the box, requiring no tedious configuration effort) and automation via integration (a complete set of free APIs and connectors enable automation to save time, improve data accuracy, and simplify data sharing).

Furthermore, Sunbird also prides itself on extreme scalability (enterprise-class scalability that can handle millions of assets, billions of data points per day, and thousands of users), data-driven collaboration (shared dashboards and team views break down organizational silos and encourage information sharing) and super-fast deployments (deployment takes half the time of first-generation tools, requires significantly fewer resources, and provides fast ROI). *sunbirddcim.com*

It's well known that **netTerrain** is a DCIM specialist, which means its solution offers strong capabilities for managing aspects of your physical infrastructure—outside plant, site maps, cable management and more. Known for being simple, customisable, and affordable, the company says its DCIM offering is a good option for data centre leaders who aren't looking for additional products, such as CMDB, data centre asset management, IT asset management, or application dependency mapping. It's also worth noting that with netTerrain, you get a GIS-compatible tool with the basic DCIM capabilities you would expect from this category of IT solutions. *netterrain.com*

The power of TETRA technology

Hannu Aronsson, TCCA's TETRA Applications Group

TETRA is recognised as a leading mobile communications technology that is delivering mission-critical voice and data services to public safety organisations and mobile workers worldwide. It is the technology upon which the UK's Airwave network is built. TETRA solutions deliver exceptional secure and reliable critical voice services but the inherently rich data capabilities of TETRA are often under exploited. The data applications described in this article are real life examples of how end users can and are reaping added organisational value from their TETRA asset investments.

TETRA supports a variety of messaging applications: plain text messaging (Short Data Service - SDS): flash text messages that appear on screen immediately; messages that can be sent to a talkgroup or individual radios, with images attached. These applications support acknowledgement features to confirm to the control room that a message has been received by the radio, and that it has been displayed to the radio user. Predefined message templates and support for forms enable quick and easy updates and reporting on the move.

Many TETRA users provide their control rooms with real-time status updates – enabled by simple one-button updates from a radio and rapid processing in the control rooms. Status and SDS text messages are standardised to ensure interoperability between all TETRA radios and TETRA networks.

TETRA radios support "callout" which provides alarms and task management information from the control room and acknowledgements from users, similar to 2-way paging. For example, Norwegian firefighters use TETRA callout to efficiently dispatch operations. Callout is a standardised feature that works across all TETRA radios in the same way. With callout, control rooms can ensure information is read and acted on quickly. There are also dedicated pager TETRA devices available.

For public safety organisations, tracking the location of first responders is a critical safety and operational efficiency requirement. TETRA radios support Global Navigation Satellite Systems (GNSS) to enable location tracking with time and distance triggers to optimise network traffic. The TETRA standard Location Information Protocol (LIP) may be used to ensure efficient location tracking on large TETRA networks with radios from multiple vendors. Location can also be sent automatically when an emergency call starts, including Bluetooth-enabled indoor location tracking and Z-axis location - i.e. height and floor information.

TETRA radio functionality can be securely controlled remotely via data messages sent from the control room. SDS or status messages can trigger actions on the radio - e.g. changing the talkgroup or making sure the audio volume is on high. Only authorised systems can activate remote control actions. TETRA networks and radios also support over-the-air stun and kill to remotely disable lost or stolen radios.

TETRA SDS messages enable essential database lookups from mobile radio users, such as a vehicle licence plate check. The Finnish police and border guards, for example, have access to their databases from TETRA radios to check vehicles and persons in the field. Information is securely always available through the nationwide TETRA network.

Supervisory Control and Data Acquisition (SCADA) solutions are used within the industrial sector to collect, monitor and automate processes. TETRA offers multiple communication methods ideal for SCADA, from status and SDS messages, to packet data for IP-based protocols. For example, power companies can manage transformer substations, oil and gas companies can detect leaks and control pipeline flow rate and mining operations can monitor heavy machinery. Many power utilities use TETRA devices to control power stations, photovoltaics, and wind generators and for distributing alarms in real time via SDS, Voice Alarm or callout.

The same TETRA radio solutions that are providing reliable voice communications for buses, subways, trams, railways and airports can also provide data applications to increase operational efficiency - e.g. location tracking, keeping passenger information displays up to date and accessing operational information from TETRA radios. New Jersey Transit and major airports in the US are using TETRA for voice, location, and other applications to optimise their operations.

Public announcements (PA) and audio alarms are key to safe operation and communication to workers inside and outside oil and gas plants. TETRA SDS messages from the control room can trigger RTUs (Remote Terminal Units) to activate sirens and play audio PA messages, to quickly alert everyone in case of a gas leak, fire alarm or other incident. In addition to data-enabled alarms, the control room operator can use a group call to specific PA systems to share any important information by voice.

In addition to audio voice accessories, there are data-enabled accessories for TETRA radios, including Near Field Communications (NFC) readers, indoor location beacon readers, gas sensors, temperature sensors and barcode readers. These accessories can send collected information and alerts over the TETRA network to the control room, using the standard TETRA messaging features. TETRA radios can also connect to on-person sensors via Bluetooth and monitor, for example, gas in the environment, heart rate or body temperature and alert the control room over TETRA if the situation becomes dangerous.

Many users carry a TETRA radio and a smartphone. To simplify operation, an application installed on the smartphone can be used to control the TETRA radio - e.g. change talk groups or perform messaging - via a Bluetooth link. For some users, like covert operatives, this also enables them to communicate over TETRA while appearing to play with their smartphone. ■

“Please meet...

Rob Steele, CEO of Iplicit

What was your big career break?

I’d have to say it was going from a paper round to being a golf caddy at 13 years old – the money quadrupled!

I used to go to my local club and sit on the wall waiting to be picked, but I was often the very last choice – as the ‘stronger’ older kids were selected by the regular players first. One day I was chosen by a group who were visiting from Iceland though and that day changed everything for me.

When they left, I remember them giving me £20. This is circa 1981 by the way, so you could imagine my shock at all this money – I tried to act completely normal, and calmly put the note in my pocket before skipping all the way home! I couldn’t believe it. To this day, it still makes me smile to think about that random but really generous moment I experienced at such a young age.

Who was your hero when you were growing up?

My dad – and Tarzan. Johnny Weissmuller was the actor who played Tarzan back then, and he was also an Olympic swimmer, which for me was legendary. I was a keen swimmer when I was younger and travelled the country competing as part of the Poole Dolphins – I wasn’t quite as great when it came to swinging from vines, however.

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

Not to take life too seriously – as you can see from this Q&A.

Which law would you most like to change?

Gun laws in the US.

What would you do with £1m?

I would invest it in iplicit – the true cloud accounting software firm I’m now CEO of. We’re entering a really exciting part of our growth trajectory with new feature releases to help alleviate the stresses and strains for mid-market organisations that have outgrown their entry-level cloud software such as Xero and QuickBook, but yet don’t want the complexity and cost of NetSuite and Microsoft Dynamics at the other end of the scale.

The mass migration to cloud systems is well underway, and as a business we are not constrained by opportunity – the only thing holding us back is recruiting enough talent fast enough. Therefore, this additional money would be used to attract more star players to our (already) phenomenal team and help more organisations to adopt the best cloud finance system on the market.

Where would you live if money was no object?

I would struggle to settle in one place – so I’d have to try at least 10, is that allowed in this Q&A? Because of my love for skiing, cycling and all water-based activities, I’m drawn to mountains and lakes so I’d instantly choose those types of surroundings.

A cosy stone-built house with floor-to-ceiling glass, open fireplaces, a private jetty and boathouse, built beside a huge lake and at the foot of snow-capped mountains behind would do nicely. I don’t ask for much do I?

And, based on all the places I’ve travelled to before, I’d probably choose somewhere like Lake Locarno/Lugano in Europe or maybe even Lake Tahoe in the US.

The Beatles or the Rolling Stones?

There’s no right answer here, but for me the Rolling Stones would edge it on most occasions. In truth, you could write chapter and verse on the merits of both of these legendary bands, so it probably comes down to what you want to listen to at the time.

The Beatles are like a fine wine; served at the perfect temperature in an idyllic setting they are just sublime. Sometimes though, all you really want is a cold beer and a greasy burger; and that’s the Stones. More often than not, I’d enjoy that cold beer.

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

Film, primarily because I like the idea of creating something special that will last many years. I could see myself developing the synopsis for a movie – most likely a comedy – and working with a scriptwriter, choosing the right cast, travelling to different locations, and editing the whole thing together sounds like it could be a lot of fun.

What’s the best technological invention in your lifetime?

DNA/genome mapping. Genomics is providing us with a human instruction manual that outlines how we go about ‘fixing’ ourselves and, while I don’t believe we should all live forever, I’d be keen to see how it might measure up when it comes to eradicating some of the horrible diseases that we have such as the many forms of cancer and dementia.

If you could have dinner with any famous person from the past or present, who would you choose?

That’s such a tough question – particularly when it comes to choosing just one. I think a lot of people might say this, but I’d love to sit down with Sir David Attenborough and just listen to what he has to say. He’s not only a ‘national treasure’, but I know he’d be truly fascinating and have some incredible stories to tell. ”