MAY 2021
networkingplus.co.uk

NETWORK+

**Moving to containers**
Achieving a modern, agile and resilient enterprise
**Chris Bujis, NS1, *p7***

**The critical comms column**
The path to transforming control rooms operations
**Rhiannon Beeson, APDC & BAPCO, *p12***

**Questions & answers...**
A chat with the co-founder and VP carrier relations, EMnify
**Alexander Schebler, EMnify, *p16***

# O2 to slash data centre emissions in 'radical overhaul'

**O2 is carrying out a "radical overhaul" of its operations in a bid to cut emissions from its data centres by more than half a million kilograms within a year.**

The British telecommunications giant said it has invested in innovative energy-efficient cooling equipment to regulate the temperature of data centres and core network sites. The new kit, which uses natural cold air outside of locations to cool inside, will replace traditional electric-powered air conditioning and transitional gas-based refrigeration.

It is being paired with energy management software provided by EkkoSense, which uses smart sensors fitted to data centre equipment to monitor how much cooling each site requires and how the delivery of this cooling can be optimised for energy efficiency.

"Our software's ability to capture and analyse O2's critical power, space and cooling information in real-time gives their data centre team access to much more powerful optimisation capabilities, as they progress towards net zero," said Dean Boyle, chief executive officer at EkkoSense."

As a result, O2 estimates that each site with the new technology will consume 15-20% less energy per annum. To date, around 70% of the operator's sites have received the upgrade. Once all sites have the technology installed, the operator forecasts, CO2e savings of more than 678,000 kilograms will be delivered within a 12-month period. The move comes after O2 shifted all sites where it manages energy bills directly to 100% renewable electricity.

"Our number one priority is keeping customers connected, but that cannot be at the expense of the environment," said Tracey Herald, O2's head of corporate responsibility and sustainability said. "Data centre cooling is a great example: the more data we use, the hotter the centres can become. Historically networks have relied on air con, but the UK has plenty of fresh, cold air that does the same job – so we're getting rid of old kit and using energy in a smarter way."

To date, around 70% of the operator's sites have received the upgrade.

Furthermore, O2 has also delivered an 82% improvement in energy efficiency across the network since 2015. However, it claims that the focus on data centres is necessary in light of the net-zero transition and the UK's growing demand for 4G and 5G. Total peak hour data traffic on the O2 network this April and May was some 55% higher year-on-year.

In 2016, it was reported that the world's data centres used more than Britain's total annual electricity consumption – 416.2TWh, significantly higher than the UK's 300TWh. This was equivalent to 3% of global electricity demand and, with the grid mix at the time taken into account, around 2% of annual global emissions.

In 2020, O2 became the only mobile network operator to commit to net zero by 2025, whilst working with supply chain partners to reduce emissions by 30% in the next five years. ■

# Cyber fears as nearly 200 devices lost

The Department for Education (DfE) has seen nearly 200 devices including laptops and mobile phones lost or stolen over the last two years, according to official figures.

Overseen by secretary of state for education Gavin Williamson, the DfE is responsible for child protection, education, apprenticeships, and wider skills in England has seen remote working surge due to the Covid-19 pandemic.

The data, which was obtained under a Freedom of Information (FOI) Act inquiry by Parliament Street think tank has revealed the number of lost and stolen gadgets since 2019.

Of the total 196 devices reported missing, mobile phones were the most common, with 145 missing in total since 2019, 22 of which were reported to be Blackberries, which were previously the default standard issue device for government officials. Last April, it was announced that the DfE had launched a free online learning platform to help people pick up digital and cyber skills while in lockdown.

"Amidst the chaos caused by the Covid-19 pandemic, there has been huge pressure on government departments to carry on providing crucial public services with staff working remotely," said Edward Blake, area vice president, Absolute Software UK&I. "However, if one of these lost devices ends up in the wrong hands, the organisation in question could be facing a far more costly predicament than first anticipated."

The DfE has so far dispatched 1.29 million laptops and tablets as part of a scheme to provide over 1.3 million devices to disadvantaged and vulnerable children and young people with devices and connectivity to access remote learning during the 2020/21 academic year.

A total of 104 phones and 35 laptops were reported as lost or stolen in 2019, while a further 41 phones and 16 laptops went missing in 2020. ■

# Arrow Electronics inks Nvidia solutions distribution agreement

Global technology provider Arrow Electronics has expanded its portfolio of business solutions for the data centre by entering into a distribution agreement with Nvidia, which enables Arrow to offer its customers Nvidia networking solutions.

Under the terms of the deal, Arrow will be one of the key distributors in the UK with access to the entire Nvidia solutions portfolio.

It will distribute the latter's high-speed Ethernet and InfiniBand solutions, which increase data centre efficiency by providing high throughput and the lowest latency, delivering data faster. The new agreement will allow Arrow to provide its customers with a broader offering and more choice.

"Modern workloads can put massive performance demands on the data centre, and Nvidia networking products provide performance, speed, low latency, high efficiency and resilience," Dan Waters, country manager of Arrow's enterprise computing business in the UK said. " Our strength as an aggregator lies in providing our channel customers with unrivalled access to complementary, best-in-class technologies. Nvidia has quite broad and well-established relationships with the largest industry vendors, all of whom also work with Arrow."

***Dan Waters, country manager of Arrow's enterprise computing business in the UK says " our strength as an aggregator lies in providing our channel customers with unrivalled access to complementary, best-in-class technologies"***

Syd Virdi, senior director of EMEA channel sales at Nvidia Networking, added: "Arrow's experience and broad customer network enable Nvidia solutions to reach a wider audience. NVIDIA InfiniBand and Ethernet networking for server and storage fabrics, Open Networking solutions for edge and cloud, and other accelerated networking solutions for AI and enterprise data analytics all offer customers the latest most advanced technology available in today's market." ■

# Royal United Hospitals Bath NHS Foundation Trust makes communications system upgrades

The Royal United Hospitals Bath NHS Foundation Trust has selected Cinos to modernise its unified communications platform.

A Cisco-powered unified communications platform will provide and combine multiple communications channels for the Trust's 6,500 employees, such as voice, video, personal and team messaging, voicemail and content sharing.

It will give staff the tools and ability to work more flexibly on site and when working remotely, including extending audio and video calls to Microsoft Teams.

"The benefits of the new platform will also extend to patients, as a new centrally managed contact centre will make it easier for them to engage with our clinical services," said Liam Abbott, chief technology officer at Royal United Hospitals Bath NHS Foundation Trust. "By improving the quality and efficiency of communications, we're making our services more accessible to those who depend on them."


***Elecupta sum qui sint voluptio explique vellaudam rest laborem quidebis utecerferum***

Providing acute treatment and care for around 500,000 people in Bath and the surrounding areas, the trust required a cloud-based platform – one that allows it quickly to scale up the service as and when needed, is able to support the integration of care services, and to connect the trust with GP surgeries, community hospitals and large-scale Covid-19 vaccination centres.

The Cinos Cloud Unified Communication service builds upon this foundation and will provide the Trust with a robust unified communications platform. Updates to the telephony system and contact centre will also lay the foundations for any future updates that the Trust requires, enabling it to easily build upon the existing infrastructure.

The roll out of the platform and service began in March 2021, with go live planned for September 2021. ■

# Wireless Logic helps Exponential-e with SD-WAN deployments

IoT connectivity platform provider Wireless Logic has been working with UK-based IT, cloud and network services provider Exponential-e to boost its SD-WAN deployments.

The latter has used the former's private network, NetPro infrastructure, combined with its connectivity management platform, SIMPro, to guarantee secure connectivity across LPWAN (NB-IoT, LTE-M), 4G and 5G.

Servicing over 3,000 companies, with customers including Virgin Atlantic, Guinness World Records and Channel 4, Exponential-e required high quality and secure cellular connectivity to further enhance customer solutions.

It also required the technical ability to integrate cellular networks directly into its core data centres via Network to Network Interface (NNI).

Wireless Logic helped Exponential-e to provide customers with a carrier grade 4G solution using Fixed Private IP and private APNs over dual dedicated NNIs for added resilience across customers' WAN infrastructure.

Rachel Gnaiah, product manager at Exponential-e, said by partnering with Wireless Logic, the company was able to provide its mobile connectivity offering not only nationally, but also internationally, whilst allowing it to enhance its "propositions within the IoT space and Industry 4.0".

***With customers including Virgin Atlantic, Guinness World Records and Channel 4, Exponential-e required high quality and secure cellular connectivity to further enhance customer solutions***

Ollie Wallington, head of business development at Wireless Logic added that the company's agnostic approach is highly valued by its customers, who look to the Wireless Logic team as 'trusted advisors'.

"This, along with our exceptional network of customers and partners, make us ideally placed to support Exponential-e's SD-WAN deployment as well as other IoT applications that use cellular as a means of communications," he added. "We look forward to working with them on this and further projects in the future." ■

# Glasgow Caledonian Uni attack not thought to be ransomware

The cyberattack on Glasgow Caledonian University on Friday May 14 has not so far yielded evidence of data theft and ransom note in the code, the institution said.

Officials described the incident, which downed IT systems, as a 'limited cyberattack', which was detected early and led to technical teams working throughout the weekend to contain its spread.

Cyber security experts have been brought in to work on the incident with support from Police Scotland, the National Cyber Security Centre (NCSC) and the Scottish government's Cyber Resilience Unit.

"Last Friday (14th May), our IT security software and staff identified that GCU had been subject to a limited cyberattack," a Glasgow Caledonian University spokesperson said in a statement. "Unauthorised access was detected early and our team worked over the weekend to contain it and limit any potential damage. There is no evidence to suggest data has been compromised, nor that ransomware is present."

As a precaution, the university said access to some limited IT systems have been restricted until a full evaluation and any necessary remedial action is completed. The spokesperson added that the university "will look to have all systems fully functional" at the earliest possible opportunity. They also said that telephone lines are temporarily affected, though students and staff will naturally contact us by email, messaging systems and calls diverted to mobile phones.

The university said all of its students have been made aware of the attack. Students wishing to contact the university in relation to this matter can still do so by emailing studentsupport@gcu.ac.uk, it said. ■

**EDITORIAL:**
**Editor: Robert Shepherd**
**roberts@kadiumpublishing.com**
**Designer: Sean McNamara**
**seanm@kadiumpublishing.com**
**Contributors: Gerry Moynihan, Steve Law, Kelvin Murray, Chris Bujis, Rhiannon Beeson, Alex Chircop, Ali Nicholl, Vik Malyala, Alexander Schebler, Raj Samani, Corey Nachreiner, Candid Wüest, Rory Duncan, Chris Goettl, Sergei Serduyk, Andrea Babbs, Mark Raeburn, Nigel Thorpe**

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

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

**ISSN: 2052–7373**

# DataVita buys Lanarkshire DC site from Fortis

DataVita, Scotland's largest data centre and multi-cloud services provider, has acquired the Fortis data centre in Lanarkshire with £45m of support from parent-company HFD Group.

The Lanarkshire site is the only one of its kind north of the border, supporting critical IT services for an estimated two million people in a country with a population of 5.5 million.

DataVita has operated the data centre since 2016 and was the facility's first occupier, providing data centre and cloud services to businesses and public sector organisations.

The purchase will also support DataVita's drive to enhance the data centre's green credentials. Earlier this year, DataVita became the first Scottish IT company to sign the Climate Neutral Data Centre Pact and announced plans to take the facility off-grid, generating its own electricity from wind and battery-powered back-up systems. It will equally support growth for DataVita and the wider interests of commercial property and investment company HFD Group.

Danny Quinn, managing director of DataVita, has often spoken of growing DataVita to five times its current size.

In 2019, the company booked a 76% increase in revenues and was appointed to the Scottish government cloud services framework, allowing it to offer public sector organisations access to a range of cloud and data centre facilities.

"We can now accelerate our plans to drive the data centre's environmental and wider ESG focus, open up new opportunities with our existing clients, and support our market competitiveness and ability to work with larger users of IT services across the UK.," said Quinn. "From a wider HFD Group perspective, it underlines our support for, and investment in, IT services for our existing and prospective occupiers."

He added that property and IT "are becoming intrinsically linked and our strength on both fronts – and ability to offer everything from businesses space to connectivity and cyber security – is a powerful offering" to businesses and public sector organisations alike.

Quinn said: "As the disruption caused by Covid-19 continues and our economy and society rely more than ever on digital infrastructure, DataVita is in a strong position to support the IT and data needs of businesses and public sector services in a secure and sustainable way."

HFD, the commercial property and investment company, is investing £45m, which includes the undisclosed purchase price." ■

*The Lanarkshire site is the only one of its kind north of the border, supporting critical IT services for an estimated two million people in a country with a population of 5.5 million*

# UK sexual health screening provider adopts Node4 cloud

Preventx, a UK provider of remote sexual health screening services, has migrated from its traditional server to Node4's Microsoft Azure-based public cloud. The business provides its services through contracts with local authorities and NHS trusts. These services are designed to make sexual health screening easier, more accessible and cost-effective. The move will give Preventx access to a resilient, cost-effective and agile infrastructure.

"We were looking to create a secure, highly available and resilient infrastructure with access to Healthcare Social Care Network (HSCN)," said Chris Jelley, chief technology officer at Preventx. "We wanted to work with a trusted provider – not only in the initial provision of data transition, but for ongoing technical support too. Node4 has a strong track record with other healthcare providers and a great deal of experience supporting Azure frameworks.

Jelley added that in the months since partnering with Node4, Preventx has seen huge benefits across its business. He said that adopting public cloud and Azure Services have delivered a flexible and agile infrastructure – "one that's far more cost-effective and strategic" than stacking and then under-utilising physical servers.

"To anyone in the health sector and beyond questioning the validity and effectiveness of public cloud environments, I'd say if you haven't made the move already, what are you waiting for?" he said.

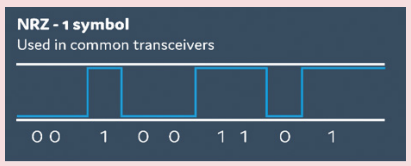
Node4's HSCN connectivity also enables Preventx to securely send and receive data from its public sector partners, which the company said is an essential part of ensuring patient confidentiality. ■

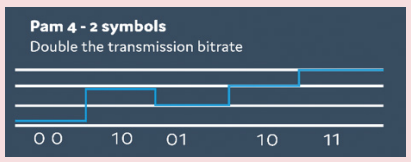
FROM THE COVER

# PAM-4: coming soon to a network near you

The coming attractions are part of the cinema experience offering an entertaining look forward towards what is on the horizon in anticipation of the main attraction. Powered by PAM-4 modulation, 400G Ethernet is now the main attraction of the networking world, offering immediate relief to a pandemic-fueled demand for bandwidth at the network core. The advent of 400G is only the opening chapter in the PAM-4 saga, which, in turn, will enable the growth in network capacity beyond the core all the way to server.

Network operators did not need to be concerned with modulation in previous network upgrade cycles. Fibre optic transceivers utilised NRZ (binary non-return to zero) formatting and their interoperability was ensured between like data rates and interfaces. From a technical standpoint, NRZ transmits 1 bit per waveform (0 or 1). In contrast, PAM4 waveforms that each can carry 2 bits (instead of 1 for NRZ). PAM4 waveforms have 4 different levels or steps, carrying 2 bits each: 00, 01, 10 or 11.




Baudrate and bitrate are equivalent with NRZ transmission, meaning the same baudrate and bitrate as one symbol can carry one bit. 25Gbps (gigabit per second) bitrate is equivalent to 25GBdps (gigabaud per second) and there is no need for further analysis. 400G PAM-4 transceivers each hand off eight 50Gbps lanes on the electrical interface to the host network element. Each PAM-4 lane carries a line transmission rate of 25GBdpd (25-gigabaud) at 2 bits per symbol to achieve 50Gbps per lane.

Network operators may look at upcoming technology transitions like the preview of a horror film: they appear scary and expensive. The transition to PAM-4 will not be without its complexities, but with the use of current transceivers, expensive massive upgrades will not be necessary. 4x100G breakout architectures have been simplified by deploying single lambda 100G DR, FR and LR transceivers. QSFP28 single lambda transceivers will interface with existing QSFP28 ports (4x25G NRZ), while interoperating with 400G breakout transceivers optically. Offering full support for data aggregation at the core, spine/leaf, and even the server for top-of-rack architectures.

Newer devices like wireless controllers and application servers will be some of the first in the wider enterprise to deploy PAM-4 SFP56 50G switch ports. SPF56 ports are backwards compatible with NRZ SFP+ or SFP28 transceivers, but network operators may need the same flexibility enjoyed with dual rate 10G/25G and 40G/100G transceivers to upgrade one side of a connection, deferring the other side until budget constraints allow. A new generation of SFP56 multirate transceivers offer the backwards compatibility to legacy 10G and 25G NRZ optical interfaces that allow for incremental upgrades network operators require.

PAM-4 is coming to a network near you. Understanding network transceiver options can be critical to ensure your network upgrade is both a low-budget and a feel-good story.

*By Ray Hagen, ProLabs Group Product Manager*

# AWS to expand cloud skills programme

Amazon Web Services (AWS) will grow the number of people across the UK with the skills needed to take on entry-level roles in cloud computing through the geographical expansion of its long-running re/Start programme. Originally launched in January 2017 with a focus specifically on equipping young people and ex-military personnel with cloud skills, re/Start has since expanded its focus to include people who have been made redundant from non-tech careers too. At launch, the firm said it hoped that up to 1,000 individuals would be given the opportunity to participate in work placements through the UK version of the scheme and several years later AWS is now preparing to launch new cohorts for the programme in Belfast and Cardiff.

# Doncaster broker in £15m attack

Doncaster-based broker One Call Insurance is the victim of a ransomware attack committed by the Darkside crew, the same cybercrime group that extorted US fuel network Colonial Pipeline earlier this month, reported the Doncaster Free Press. The local paper said hackers demanded £15m from the broker and - if this was not met - the group threatened to publish the firm's data, which includes customer data such as passwords and bank details. A statement reads: "On 13 May, we began experiencing some disruption to our IT systems. Since then, we have been working with a dedicated team of forensic specialists to restore our systems and investigate the situation."

# Hacking up 300% - NTT GTIR report

NTT launched its annual Global Threat Intelligence Report (GTIR), which found up to a 300% increase in attacks on specific sectors and types of software in the move to remote and digital services. It highlighted cyber-opportunists seizing on the effects of the pandemic, who committed major attacks on the healthcare, manufacturing, and finance industries, with 200%, 300% and 53% increases, respectively. It also showed a 41% impact from cryptocurrency miners on all detected malware globally. Cryptominers have replaced spyware as the most common malware in the world.

# CityFibre could expand fibre rollout

CityFibre could expand its full fibre rollout to 10 million businesses and homes across the UK if it completes the sale of a 30% stake in the company to a private equity firm. The company's two major shareholders – Wall Street Infrastructure Partners and Antin Infrastructure Partners – control 70% of the company. However, according to The Mail on Sunday, CityFibre is nearing a sale of the remaining 20% for £1 billion. CityFibre does not offer any direct-to-consumer products but instead delivers wholesale services to broadband providers, such as TalkTalk and Vodafone, and to mobile operators who require fibre backhaul for their mobile sites.

# 'European organisations prepared to embrace AI', says Juniper

Research from Juniper Networks has found a growing appetite from both enterprises and consumers to use AI technologies. It surveyed 700 global IT decision-makers for its research and found that most (67%) executives have AI as a top strategic priority for 2021. Some 95% of the respondents believe their organisation would benefit from increasing the use of AI in their daily operations. Meanwhile, 82% say it makes employees more productive, while 74% say it improves staff happiness. However, integrating AI remains a challenge, with 73% of respondents claim their organisation is struggling with adoption due to issues preparing and expanding their workforce to integrate AI systems.

# Neos launches unified comms services

Neos Networks has launched its cloud-based Unified Communications as a Service (UCaaS) solution, which is a cloud-based communications and collaboration platform. It includes contact centre capability and is fully interoperable with other solutions including Zoom and Microsoft Teams. This interoperability provides ease of use for organisations that already have existing conferencing tools but are looking to either add functionality or gradually replace their existing set-up. The UCaaS package offers high levels of security, compliance, and reliability – as well as an intuitive, centralised management portal. The easy-to-use portal acts as a go-to hub to proactively monitor all call features and admin management to ensure the smooth-running of scheduling and organising meetings. This will enable IT teams and end-users to have a simple user experience that gives them full visibility of the performance of the service, the company said. The announcement forms part of the firm's growth strategy, including products and the size of its network.

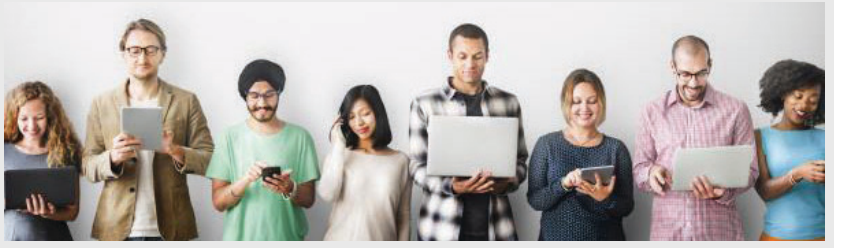
# 'Remote workers put data at risk'

More than a third (35%) of UK IT decision makers admitted that their remote workers have already knowingly put corporate data at risk of a breach in the last year, according to an annual report from Apricorn. This is compounded by the fact that given over one in 10 surveyed IT decision makers also noted that they either have no control over where company data goes or where it is stored (15%) and their technology does not support secure mobile/remote working (12%). Additionally, more than half (58%) still believe that remote workers will expose their organisation to the risk of a data breach. GDPR compliance was the third biggest concern with 32% of organisations highlighting that mobile/remote working makes it harder to comply with GDPR, compared with just 16% in 2020.

# Crossword buys VCL

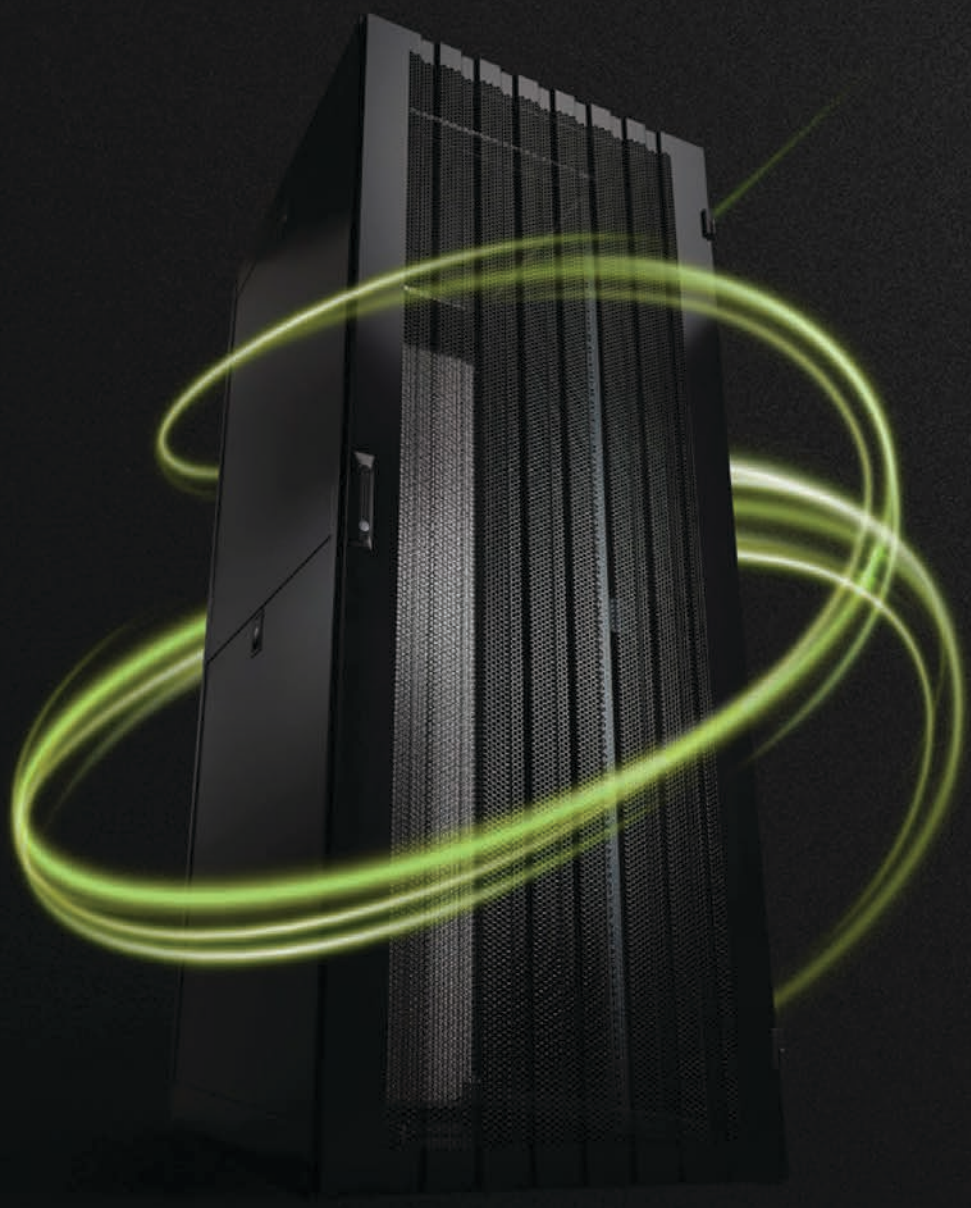
Crossword Cybersecurity has acquired Verifiable Credentials Limited (VCL) in a deal worth up to £2.75m. VCL is the provider of Identiproof, the World Wide Web Consortium (W3C) verifiable credentials compatible middleware and wallet technology. Identiproof is a central technology in applications for the issuing of digital certificates and documents that cannot be forged or transferred and that respect the privacy of the holders of those certificates. It does this through the process of selective disclosure, whereby the recipient requests the minimum of information in conformance with GDPR. Crossword said the payments are made up of cash and company shares.

## Word on the web...



# 'Building your pipeline' – a raft of key tips from CNet Training

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



# BIG ON CHOICE

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

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

excel
without compromise.

# Going under the radar

## Paolo Passeri, cyber intelligence principal at Netskope, explains how 50% of network traffic flies go undetected by legacy security defences

It is no secret that cloud is at the heart of modern IT and digital transformation, enabling a lot of freedom – freedom to do things when we want, where we want. However, it does come with a price. Opening systems up to be accessed anywhere, from any device, has meant that the lines of control and access have blurred and 50% of traffic can go unseen by legacy security defences.

### From technological concept to technical reality

According to findings in Netskope's February 2021 Netskope Cloud and Threat Report, the number of cloud apps in use per organisation increased 20% in 2020. It found that organisations with 500 - 2,000 employees now use, on average, 664 distinct cloud apps per month.

This mass adoption of cloud was well under way a year ago, but over the past 12 months, cloud services have proved themselves to be invaluable. When 2020 arrived, CIOs found cloud to be a conveniently rapid and outsourced method of responding to the immediate challenges of mobility and the multichannel provision of resources and business tools – critical just to enable business as usual to continue during the pandemic. The result of lockdown, and the hasty adoption of cloud, is an unprecedented number of people working outside of traditional organisational IT perimeters and therefore outside of the protection of traditional security defences.

At the beginning of the pandemic, the primary concern was to provide business continuity and enable everyone who could to work from home; security considerations were secondary. Traditional security strategies tend to focus on protecting the data centre and the network, and so the overnight relocation of employees and applications outside of that perimeter left sensitive data at serious risk of falling into the wrong hands.

Cybercriminals are smart and move quickly if they spy a weakness or opportunity. The rapid growth in cloud adoption without cloud security strategies being implemented at the same pace, has left the door open for cybercriminals to abuse popular cloud services. They have used many techniques over the past year to successfully evade legacy security defences and target trusted cloud apps that are open to phishing and malware attacks; 61 per cent of all malware is delivered via a cloud app, up from 48% year-over-year and cloud apps are now the target of more than one in three (36%) phishing campaigns.

Because the endpoint is at risk of being compromised via personal traffic such as a phishing email received via a personal mailbox, or malware injected visiting a non-business website, these types of attacks can have devastating consequences for businesses. Put simply, a compromised endpoint can be used as a foothold to break into an organisation's systems.

Another danger is that, as work and home life continue to blend, it is now much more common for employees to use the same device, whether it's personal or corporate, to access both personal and business content in both personal and business instances of cloud applications. Some 83% of users are accessing personal apps on corporate devices, and the average enterprise user uploads 20 files to personal apps each month from the same managed devices. This is leading to a growth of sensitive data in personal apps, greatly increasing the likelihood of data being mishandled or leaked.

Behind these risks is a very simple technical reality - the Internet has changed. Cloud activity now represents 53% of secure web gateway traffic and uses a new API or JSON language. It is everywhere, and to be effective, any security tool needs to be able to interrogate API and JSON data (which is not the case for most legacy systems) and it needs to be able to make sense of both content and context.

### What needs to be done?

Today, the majority of companies subscribe to, or maintain, security solutions that secure less than 50% of traffic. They are limited to policing html web traffic but if we are to secure the cloud, we need an understanding of these new languages. And because of the nature of cloud access, this is something that can only be done in the cloud, via the cloud (you simply cannot police the movement of data between a personal and a corporate instance of the same cloud app). Businesses need to ensure that they have visibility of the content and context of cloud application use, and that they are able to apply granular policy controls if they want to make use of the productivity tools that are central to their IT, without leaving themselves exposed to risk of attack by cybercriminals.

It is clear that the lines of control and access have blurred and the user is the new perimeter. This new approach is the primary driver behind the growing adoption of a SASE (Security Access Service Edge) architecture - a paradigm that sees the convergence of the network-as-a-service and security-as-a-service concepts and aims to enforce security policies at the edge, where users access and manipulate data, whether it's a website or cloud application, regardless of the access method.

Now that this remote working trend has consolidated, business stakeholders and IT teams must work together to enable an agile remote workforce without sacrificing productivity, user experience or security. The shift from thinking that the perimeter is a physical boundary to taking a user-centric approach does not need to pose new risks to organisations. That's why in the new architectural model, security is enforced at the access edge, regardless of the access method or device classification (corporate or personal), and organisations are able to secure 100% of their data. ■

*Paolo Passeri, cyber intelligence principal at Netskope*

# LinkIQ™ combines Fluke Networks' Cable Performance technology with Switch diagnostics for trusted cable testing

The LinkIQ™ Cable+Network Tester (LinkIQ) simplifies network troubleshooting when building or maintaining networks. Rugged, reliable and accurate, it features a gesture-based touchscreen. It combines switch diagnostics with state-of-the-art cable measurement technology to enable professionals to troubleshoot network cabling and/or connect Power over Ethernet (PoE) devices to the network and provides simple pass/fail test reports using the company's innovative LinkWare™ PC Cable Test Management Software. It can verify the performance of switches.

"New technologies such as 10 Gb/s Ethernet and expanded Power over Ethernet are at the core of today's networks," said Walter Hock, Vice President Products of Fluke. "Whether it's an installer who needs to ensure error-free operation and document their work or a trouble shooter supporting advanced devices, they both need a tool that combines support for today's advanced technologies with an ease of use that saves time and a price that means it can be widely deployed."

### Single-Test

The LinkIQ is based on a single-test approach that automatically provides the appropriate measurements based on what is at the other end of the cable.

### Simple reporting

The LinkIQ uses LinkWare™ PC, Fluke Networks' reporting software which supports a variety of testers going back 20 years and is the industry's de facto standard reporting solution with tens of thousands of active users.

### Specific Feedback

"The LinkIQ is professional, intuitive, easy to use and very quick to return results. The device has an easy-to-read screen and delivers a precise bullet point summary of key information," said Russell Queenan of Thorntons Communications. "The real benefit of using the LinkIQ was the ability to challenge the capability of the old CAT5 cabling that we had not installed. This allowed me to advise the customer about which switch to upgrade based on those results.

I knew it was good for 5G speeds, but anything above that then the sockets, cabling and patch panels would need upgrading. The notetaking and reporting functionality of the LinkIQ is extremely valuable."

### Dual-Purpose

Martin Whitefoot, Project Manager at Splice Group said: "We used the LinkIQ for large installs to verify structured cabling from point to point, to test the correct ID terminates it, or to check the speed of the cabling. The LinkIQ tester is user friendly and it performs the job of two devices that our staff would have used previously, which saves time and costs."

*Read more on the LinkIQ here*

*For more information about the LinkIQ Cable+Network tester, look here*

# Moving to containers

*Chris Bujis, EMEA field CTO, NS1*

Network teams have a lot to do to achieve a modern, agile and resilient enterprise. They must apply automation practices to speed up network management and keep pace with their DevOps counterparts. This involves solving IP assignment and internal DNS management issues that crop up as workloads migrate to multi- and hybrid-cloud infrastructures and finding more economical, agile ways to scale the infrastructure that delivers these network services — whilst simultaneously being good partners with the IT and business teams.

Increasingly, reaching these goals means shifting away from a traditional appliance-based approach for delivering network services to enabling the use of containers. They are the next natural step in the enterprise transformation strategy.

From our dealings with customers, we see that the adoption of containers is moving quite slowly and that both complexity and cultural changes are often cited as the most challenging issues in using and deploying containers. It seems that businesses are happy to put a toe in the containerisation water, but hesitant to plunge the entire enterprise in.

Containers have been widely adopted by DevOps teams to deploy and operate applications quickly. But in the networking community there is a greater degree of perceived complexity and often a lack of knowledge and this threatens to hold enterprises back.

So, what are the benefits of containerisation for network teams? Firstly, by delivering DDI infrastructure as containerised software and automating processes with infrastructure as code, the network team has more deployment flexibility and additional opportunities for automation and integration.

This is important to today's enterprise which is looking to make its legacy and owned environments operate in a more cloud-like manner by introducing private cloud and similar technologies so it can fully embrace operational velocity and automation.

The advantage of containers is that they can deploy on any platform — public cloud, private cloud, physical devices, and even virtual machines. Whether an enterprise is using cloud-based data centres, colocation facilities, or private-cloud networks the team will get more flexibility from a container-based delivery approach when it comes to choosing where and how containerised software runs, a major bonus if network topologies widely vary.

Containers also offer a lightweight footprint. Unlike virtual machines, all containers share the host system's kernel and require minimal resources to operate. They can be spun up quickly on devices with a smaller footprint than traditional hardware or virtual appliances can. This also helps to reduce provisioning and certification times, as well as automate the provisioning of a sandbox environment within needed time frames to deliver critical updates to users.

Since container deployment is programmable and quick, it's easy to spin up and deactivate containers in response to demand and, as a result, rapid auto-scaling capabilities become an intrinsic part of business applications. Organisations that regularly run live events or conferences, for example, can be fully supported by containers for temporary locations. In fact, many test or sandbox environments are so short-lived that they last for less than 24 hours.

For network teams, it can be frustrating when the time taken to deploy and update a legacy appliance is longer than the time it's actually in operation. The increasing use of microservices architectures for digital transformation also drives the ephemeral nature of enterprise production environments.

Containerised microservices simplify and accelerate deployment to the point where autoscaling capabilities can become an intrinsic part of business applications. Individual services can be programmatically replicated or decommissioned to adjust capacity within minutes. This adds to the requirement for IP and DNS updates at higher rates.

Containers can also help enterprises redefine the economics of DDI software licensing. They make it easier to scale up network services for short time frames or temporary locations without worrying about reaching appliance resource constraints or artificially imposed limits by licensing. And there's no need to incur appliance provisioning and deployment costs and delays to scale up for high-volume periods, such as Black Friday or year-end reporting.

One final benefit that must not be forgotten is that since zero trust eliminates the traditional perimeter, containers allow for an automatic zero trust compliant environment. They also mitigate the impact of a DDoS attack as an organisation can spin up new resources to absorb the increased workload.

As enterprises modernise their applications, network teams also need modern infrastructure to deliver network services for those applications. To make a real difference, modern application delivery requires containerisation supported by a DDI solution that is platform-agnostic, software-defined and scalable.

The best approach for network teams is to work with a provider that enables the transition from static network infrastructure with 'big bang' upgrades to continuous delivery of software-defined network services. They can use the same automation tools and infrastructure constructs as their DevOps counterparts. With cumbersome appliance upgrade paths replaced by deployment processes automated through API's, enterprises will accelerate deployment velocity and improve efficiency, without the overhead associated with managing traditional appliances.

# Held to ransom

**Ransomware attacks in the UK continue to grow at an alarming rate, as cybercriminals target everything from government agencies to high-net-worth individuals and blue chip corporates to small businesses. Robert Shepherd asks the experts why this is and what enterprises can do to thwart the bad actors**

## IT'S ALL ABOUT THE MONEY

### Why are we experiencing a large rise in ransomware attacks?

***Raj Samani, chief scientist and McAfee fellow:*** Over the past year, we've seen security threats and ransomware attacks continue to evolve in complexity and increase in volume. This is because cybercriminals have quickly and effectively pivoted their tactics to take advantage of the pandemic or poor cyber hygiene. As a result, enterprises endured more opportunistic COVID-19 related campaigns among a new cast of bad-actor schemes. For example, at the end of 2020, we saw a continued increase in threats from Q3 (+240%) to Q4 (+114%), with ransomware increasing by a staggering 69%. Equally the rise in open RDP to the internet has compounded the issue.

***Corey Nachreiner, CTO, WatchGuard Technologies:*** For cyber criminals, it's a bit of a no brainer. With low risk, high returns and virtually unlimited supply of victims, why wouldn't you? The other factor is the arrival of Ransomware-as-a-Service (RaaS), which increases the scale and volume of attackers. The technical risk is the same, but RaaS greatly lowers the bar of criminal actors who can launch a ransomware attack. Since the RaaS seller has already done the hard work of technically creating and designing the ransomware, even unskilled criminals can make some money by outsourcing that technical effort.

***Candid Wüest, VP cyber protection research, Acronis:*** Ransomware is profitable. As ransomware operators improve their software, and find better extortion techniques, ransomware becomes a preferred method of cybercriminals to make money. Combine this with higher accessibility through ransomware-as-a-service operations, and even less technical criminals can earn a quick pay-out with ransomware.

***Rory Duncan, GTM leader, security, NTT:*** There are currently over 1,800 variants of ransomware, with the top 45 variants reportedly bringing in the most ransom money. Over the last year, cybercriminals have capitalised on global disruption to launch sophisticated ransomware attacks on healthcare providers, governments and critical national infrastructure. While large state-sponsored attacks continue to grab the headlines, however, organisations of all sizes shouldn't let these breaches distract them from threats closer to home.

"In fact, one of the reasons that there has been such a significant rise in ransomware attacks is that they are easier than ever for cybercriminals to launch. At the end of last year, for example, our research highlighted the growing trend of Ransomware-as-a-Service (RaaS) – a business model that involves cybercriminals selling or leasing ransomware platforms to those looking to benefit financially from disrupting a company's operations.

"These platforms are becoming more and more accessible. Some of the RaaS options on the market, for instance, are targeted at novice hackers who don't even need to know how to get onto the dark web to find the latest platforms on offer. Not only that, several of the malicious entrepreneurs use social media and other sources such as YouTube, Vimeo and Selix to advertise and demonstrate how to use their products.

"With these tools readily available to hackers of all levels, it shouldn't come as a surprise that ransomware attacks are an increasingly attractive option. While results with simple RaaS platforms are, indeed, mixed, those that are successful in launching attacks have increased ransom demands. Unfortunately, some are even practicing double exploitation of their victims – demanding a ransom and still releasing the victims' personal data for sale on underground forums after they have paid.

***Chris Goettl, senior director of product management at Ivanti:*** One thing to keep in mind about ransomware is that, for threat actors, it is a business. And ransomware has a very effective go-to-market strategy and high return on investment compared to many other forms of cybercrime. Threat actors can either develop their own ransomware tools or utilize Ransomware as a Service (RaaS) solutions to quickly enter the market with a high level of sophistication. Modern ransomware attacks now typically include data exfiltration, so threat actors have many points of leverage to try and get a payout. For example, victims may pay to get decryption keys or keep their data private. And even if they don't pay, hackers can possibly sell their data on the dark web.

In thinking through ransomware attacks in this way, it becomes very clear why threat actors have been so successful in the past couple of years and why ransomware is an intensifying problem for all organizations. There are more players in the ransomware space than ever before. And the average ransom is not the $500 Bitcoin that it used to be. On average, organisations pay $233,217 and suffer 19 days of downtime following a ransomware attack.

***Sergei Serduyk, VP of product management, Nakivo:*** Even though a popular saying suggests otherwise, some crime does pay. A ransomware attack is a highly profitable crime the frequency of which has increased manyfold since the start of the Covid-19 pandemic. Sensing the vulnerability of organisations adjusting to the work-from-home reality, the attackers explore additional opportunities to make money illegally. The trend is exacerbated by the rise of cryptocurrencies, which offer an anonymous means of payment. The frequency of ransomware attacks is only going to accelerate if organisations don't improve their cybersecurity posture and ensure that they don't need to pay criminals to get their data back.

***Andrea Babbs, UK general manager, Vipre:*** The United Kingdom's National Cyber Security Centre (NCSC) handled a record number of cybersecurity incidents over the last year, a 20% increase in cases handled the year before. Cyber criminals took advantage of the Covid-19 pandemic, targeting vulnerable employees working on personal computers or open networks, who were working harder, faster and longer hours than ever before. The help and support from those in IT is not so immediate. Now more than ever, the responsibility must be reinforced throughout the entire business. Unfortunately businesses often pay the ransom, and if they pay once they will pay multiple times. A successful ransomware attack can be used various times against many organisations, turning an attack into a cash cow for criminal organisations.

***Mark Raeburn, managing director at Context, part of Accenture Security:*** Ransomware has been on the rise for the past few years and is what keeps many CSOs and CEOs awake at night. Accenture's Cyber Investigations and Forensic Response (CIFR) reported a 160% year over year (YoY) increase in ransomware events in 2020. There are many factors behind this but over the last year, Covid-19 has made things far more complicated for cyber security professionals, while presenting new opportunities for bad actors. Remote working opened the door to targeting individuals' vulnerabilities, and we have seen endless new ransomware lures and traps that imitate credible sources involving Covid-19 advice or actions.

***Nigel Thorpe, technology director, SecureAge Technologies:*** Ransomware is still easy pickings - organisations are woefully open to these attacks. Cybercriminals can either target one or a select number of organisations - or even individual people, or they can take a scatter-gun approach. Broadcasting attacks tend to lead to smaller individual receipts for the cybercriminal, but ransoms soon mount up. The more targeted attacks select organisations where loss of their IT systems will lead to major problems - like the Colonial oil pipeline in the US or the Irish Health Service attacks. In these kinds of cases there's a high probability of the ransom being paid. And if you're the cybercriminal it is still highly unlikely that you will get caught. We still see frequent attacks but no arrests. Law enforcement in this whole area needs to start making an impact.

## TAKING ACTION

### What's the first thing an enterprise should do if it is subjected to a ransomware attack?

***Rory Duncan, GTM leader, security, NTT:*** Having a thorough incident response plan in place is crucial for business continuity – and this should be first place you look if you find yourself on the receiving end of a ransomware attack.

"A successful proactive incident response plan involves a number of key components. Defining the incident response team and their roles and responsibilities, alongside identifying any skillsets that do not exist within your organisation, should be the first point of action. Outlining the communication process for during and after the incident is also important – this includes clearly defining when to alert industry regulators or law enforcement. In addition, laying out the criteria for declaring exactly when an incident has started and ended is critical. Documenting the incident from start to finish, including dates and times, should also be included within the plan, as any information about the attack is pertinent for reporting the crime and using in future training programmes.

"Your plan should also include practical processes for mitigating the attack, which can be broken into three phases: containment, removal and restoration and recovery. During the containment phase, the focus should

be on limiting the scope of the attack and preventing any further damage. The removal and restoration stage involves taking the appropriate steps to remove malicious content from affected systems. Lastly, as part of the recovery phase, you should test and verify that the compromised systems are clean and fully functional.

"When it comes to ransomware attacks, it's safe to assume that at some point your organisation will suffer a breach. With our 2021 Global Threat Intelligence Report finding that 58% of organisations feel unprepared for a malware attack, however, it is clear that more needs to be done to educate businesses of all sizes on how to react when they fall victim. Developing an incident response plan is a good place to start - if you do not already have one, now is the time to write it and embed it in everything you do.

***Nigel Thorpe, technology director, SecureAge Technologies:*** As soon as a ransomware attack is identified, pull the plug! At this stage you're unlikely to know any details so you need to stop the infection spreading. So, powering off machines and unplugging networks is a good first step. If nothing else this gives a breathing space so you can plan your next steps, most likely bringing up one machine in a 'safe mode' to start to identify the problem and plan remedial actions.

***Sergei Serduyk, VP of product management, Nakivo:*** The immediate response to a ransomware attack should be the isolation of the affected systems. By removing the infected devices from the network, it is possible to stop the spread of ransomware. In addition to containing the spread, the isolation can also help disrupt the communication between ransomware and cybercriminals. The disruption of communication is essential because cybercriminals might use it to steal or destroy infected data.

***Candid Wüest, VP cyber protection research, Acronis:*** In the case of a ransomware attack, it can be natural to think about shutting down the affected system immediately. The problem with this is that you may lose logs that can help you identify the attacker and attack vector. It is important to collect the ransom note, and relevant logs, but before that, the system should be taken offline by unplugging network cables and shutting off Bluetooth and WIFI. IT and security teams should immediately separate systems from the network and begin looking for signs of ransomware on other systems.

***Raj Samani, chief scientist and McAfee fellow:*** When a business finds itself victim to a ransomware attack, it may be tempted to pay up since it's not just the encryption that will cause concern but also the threat of leaking data. In such instances, the victim companies are encouraged not to pay the ransom. There is no guarantee that payment will result in the return of data and access or prevent the sale of sensitive data on the dark web. Instead, businesses should use the No More Ransom portal as the first port of call to determine if a decryption tool exists when impacted by ransomware.

***Chris Goettl, senior director of product management at Ivanti:*** The first step is always to understand your situation. Depending on when and how the attack was detected, this could be a very tight window. Get to a sufficient level of detail to communicate to leadership and activate the right level of response. Isolate affected areas and work to contain the spread.

The US Office of Foreign Assets Control (OFAC) also recently released an advisory stating that any company that is subject to a ransomware attack should engage with the proper law enforcement authorities and must adhere to economic sanctions and federal guidance. Many cyber gangs are nation-state backed and so paying them can violate OFAC guidelines, subjecting businesses to legal repercussions and potential fines if they pay up, as well as potentially encouraging further attacks.

***Corey Nachreiner, CTO, WatchGuard Technologies:*** Immediately disconnect infected computers, laptops and other devices and consider turning off your Wi-Fi, disabling network connections and disconnecting from the internet. Hopefully, you have backups and an incident response plan in place to define roles and responsibilities of staff and third parties. But before you start to restore data, make sure your backups are free from any malware. You will also need to reset credentials including passwords - especially for administrator and other system accounts - but don't lock yourself out of systems that are needed for recovery.

***Mark Raeburn, managing director at Context, part of Accenture Security:*** The first piece of advice is not to panic and take a deep breath – it has happened to many organisations before and it doesn't mean your business is going to make the headlines in tomorrow's news. You may want to consider calling in external experts. In many cases, a specialist security firm with experience in cyber incident response will be more adept at dealing with this kind of incident than your internal IT teams may be. They can help to identify how the attack occurred and build a comprehensive understanding of the intrusion and measured impact. This is critical during and after the incident to inform defence posturing, comprehensive take-back planning in a domain compromise and safe recovery of business operations.

***Andrea Babbs, UK general manager, Vipre:*** Contain it and report it. Our advice in this type of situation is always to work with the authorities to try to rectify the issue and follow their guidance – they are the professionals with the experience to manage the outcomes, which are hopefully towards the positive. Often, many ransomware attacks go unreported - and this is where a lot of criminal power lies. By the time a ransomware attack has been successful, the opportunity for prevention has unfortunately passed. VIPRE's advice is always 'prevention is better than cure'. But damage limitation and containment are important right from the outset. Most organisations should have a detailed disaster recovery plan in place and if they don't, they should rectify this immediately. The key to any and every disaster recovery plan are backups, as once the breach has been contained, businesses can get back up and running quickly and relatively easily, allowing maximum business continuity. As soon as the main threat has passed, we would recommend that all organisations conduct a full retrospective, ideally without blame or scapegoats, and share their findings and steps taken with the world. Full disclosure is helpful - not only for the customer, client or patient reassurances, but also for other organisations to understand how they can prevent an attack of this type being successful again.

## WHO AND WHAT CRIMINALS ARE TARGETING

### Is ransomware more of a problem for enterprises or high-net-worth individuals?

***Nigel Thorpe, technology director, SecureAge Technologies:*** Ransomware is generally more of a problem for enterprises simply because they manage more data that is sensitive than high-net-worth individuals. Organisations also use their IT infrastructure to manage their entire business, through the whole supply chain and, for example, if you own an oil pipeline network, then this too is managed via IT systems. There have been many stories over the past few years of organisations that have been severely hampered through ransomware attacks. And in the case of healthcare, people's lives are at risk when IT fails. If law enforcement bodies start to make an impact on cybercriminals targeting organisations then it is likely that high-net-worth individuals will become more attractive targets because they will want to keep their private information private while not appearing in the public gaze as a result of actions that could be seen as foolish.

***Candid Wüest, VP cyber protection research, Acronis:*** Nobody is exempt from ransomware attacks. Most ransomware operators only care about the money they can make from the attack, which means that they will go after enterprise targets just as readily as individuals with a high-net-worth. The advantage attackers have in an enterprise environment is the larger human element at play. They can spam enterprise email addresses with a bad link or document used to install and run the ransomware, and it is much more likely they will find someone who will interact with it.

***Raj Samani, chief scientist and McAfee fellow:*** Many of the recent large ransomware attacks are what we would regard as big game hunting - in other words, attacks targeting large enterprises because their ability to pay exorbitant ransoms are considerably easier. However, this does not mean that cases of groups targeting individuals have gone away.

***Corey Nachreiner, CTO, WatchGuard Technologies:*** While every day we hear about ransomware attacks on large enterprises due to the obvious impact and data protection regulations that require a company to disclose such attacks. We hear less about high profile or high net worth individuals, but we can assume these attacks are just as prevalent but simply kept under wraps – whether ransoms are paid or not. For the ransomware criminals, they can target specific organisations or individuals or simply take a scattergun approach and see who bites.

***Chris Goettl, senior director of product management at Ivanti:*** Large enterprise and high net worth individuals make headlines more, but ransomware targets a lot of small businesses. More than half of ransomware attacks target sub 1,000 size companies. The smaller organizations are often disproportionately targeted because they do not have as much financing, staffing or expertise to repel sophisticated cyber threats. For smaller organizations, a payout may even be more likely because their choices could be to pay or close their doors forever.

***Mark Raeburn, managing director at Context, part of Accenture Security:*** Ransomware is a familiar and favoured threat tactic of cybercriminals and traditionally, has been about gaining access to systems, encrypting or stealing data – which could equally target an enterprise, celebrity or high earner.

But more recently, we've seen ransomware take on a more sinister turn. Attackers are getting onto enterprise networks and staying there. They aren't just encrypting data; they are threatening to ruin a company's reputation by letting everyone know they have taken it. We are also seeing an increase in ransomware specialists. For example, there might be someone offering Ransomware as-a-Service from the dark web. That person may sell the service to someone who gets access into the organisation and makes it encryption-ready. Then, they may pass on that information to someone who is an expert in hunting and seeking out what can be monetised. Suddenly, you've got a team that knows what to look for, how to find it and how to move laterally around the organisation all working together.

***Andrea Babbs, UK general manager, Vipre:*** With the increasing number and more innovative nature of cyberattacks, businesses of all sizes must prioritise cybersecurity. Whether a business is a start-up or a larger corporate organisation, all companies are at risk of a cyber-attack. We often see multi-million pound enterprises on the news when they suffer from a data breach, such as Estée Lauder, Microsoft and Broadvoice. Different sectors are targeted for different reasons, such as the highly sensitive Intellectual Property (IP) stored by pharma organisations, or the sensitive and confidential nature of data handled in financial institutions.

But, no organisation is too small to target, including small and medium-sized businesses (SMBs), who are the target for an estimated 65,000 attempted cyberattacks every day, according to new figures. Unfortunately, these types of businesses may not have the same infrastructure and resources in place to survive such attacks, as it is found 60% of small companies go out of business within six months of falling victim to a data breach or cyber attack.

No matter the size of an organisation, the effects of a cyber attack can be devastating financially, as well as having longer-term damage to business reputation. Small businesses remain at the same level of security risks as those which are larger. Nevertheless, SMEs can safeguard their data and themselves from these types of attacks by investing in their cybersecurity and being conscious and informed of the threats they face.

# WHY CRIMINALS CONTINUE

## With so many security tools at our disposal, how do criminals continue to hack so effectively?

***Candid Wüest, VP cyber protection research, Acronis:*** Cybercriminals have time and patience on their side, as well as often having a significant budget for development of new tools. Defenders are often limited in their budgets and labour hours, putting them at a disadvantage against the adversaries. Even with the best defence tools, human eyes and intuition must still be used to effectively defend against attacks.

***Andrea Babbs, UK general manager, Vipre:*** Cybercriminals are becoming more advanced and innovative in their tactics. We have seen an increase in fileless attacks which exploit tools and features that are already available in the victim's environment. These can be used in combination with social engineering targeting, such as phishing emails, without having to rely on file-based payloads.

Bad actors are also able to spot weaknesses in workforces, particularly preying on those who are working from home as a result of the ongoing pandemic, away from their trusted IT teams. In fact, a recent survey found that 90% of companies faced an increase in cyber attacks during COVID-19.

It is no surprise that hackers use humans to their advantage, as according to data from the UK Information Commissioner's Office (ICO), human error is the cause of 90% of cyber data breaches. Humans make mistakes – stressed, tired employees who are distracted at home will make even more mistakes. Whether it's sending a confidential document to the wrong person or clicking on a phishing email, no organisation is immune to human error and the damaging consequences this can have on the business.

IT and data security is a multi-faceted, complicated area, and one which must receive investment in each layer, from the technology to the people to the tools we give to the users. If you do not have the right technology in place to keep your data safe, then you will face problems – but the same goes for having the right tools and training available to your users. Data security is a difficult and never-ending task, one which requires ongoing investments on multiple fronts by every organisation in the world.

***Chris Goettl, senior director of product management at Ivanti:*** Threat actors only need to find one weak point to gain a foothold and from there they can find the next weakness and the next, whereas security professionals must defend against a variety of weaknesses that are never ending.

Plus, hackers do not use a single attack method; ransomware attacks are sophisticated and multifaceted. In many cases, ransomware attacks behave much like advance persistent threats (ATPs). The attacker will exist within an organization for months typically. They will map out the environment, identify what workloads and systems will have the most impact on the organization and they will find sensitive data to exfiltrate. Once they are prepared, they will launch the encryption portion of the attack, but by then it is often too late.

Social engineering, email phishing, and malicious email links are major vectors that criminal organizations use to infiltrate environments and deploy malware. Unpatched vulnerable software also leaves organizations unprotected from malicious cyber threat actors exploiting known threat vectors to get a foothold into connected endpoints and then move laterally up the cyber kill chain to evolve into an ATP. In fact, this year's Verizon DBIR report noted that attackers continue to exploit older vulnerabilities, and that patching performance in organizations has not been stellar. While patching technologies have existed for years, many companies still struggle with vulnerability remediation.

***Corey Nachreiner, CTO, WatchGuard Technologies:*** You can put in multiple layers of security to protect from ransomware attacks, but it is no secret that humans are the weakest link in any security strategy. Recent Verizon Data Breaches Investigations Reports suggest that some 90% of breaches start with a phishing or social engineering attack. Most of the investment in cyber security over the last 10 years has been focused on securing computers and networks through technical defences, but as we have got better at patching and preventing IT vulnerabilities, the cybercriminals have focused more on exploiting human weaknesses.

***Mark Raeburn, managing director at Context, part of Accenture Security:*** Ransomware has become a very lucrative and low-risk activity for criminal groups, who are investing large amounts of money honing their trade. Phishing continues to be the most common infection vector for ransomware and the sophistication and sheer volume of emails and texts will inevitably catch some people out. Other methods of infection include drive-by attacks or watering hole attacks, where attackers infect popular sites with malware.

***Nigel Thorpe, technology director, SecureAge Technologies:*** The main problem is people. As soon as a person is involved the opportunity for misjudgement or mistake is huge. Most people are not - and should not be expected to be - IT security experts. Cybercriminals are well aware of this and create tempting and targeted 'bait' that appears to be legitimate. For a well-constructed phishing attack there should be no shame on behalf of the individual who clicks that link - the security system should have prevented any potential damage in the first place. However, most organisations continue to use mainstream cyber security tools, which over time have become highly complex. And where there is complexity there will undoubtedly be security gaps, misconfigurations and mistakes.

***Raj Samani, chief scientist and McAfee fellow:*** We have to recognize that there are still multiple ways to detect a potential ransomware attack. Typically, attackers use entry vectors that have been well documented, and once inside the environment there are behaviours that can point towards compromise. Of course, the challenge for any organisation is to identify these indicators in the sea of alerts they have to contend with every day.

# WHAT CAN BE DONE

## Is stopping ransomware just a case of shifting from detection to prevention?

***Sergei Serduyk, VP of product management, Nakivo:*** Yes. In the case of ransomware, an ounce of prevention is worth infinitely more than a pound of cure, which often comes in the form of a ransom. Rather than paying an exorbitant ransom, organisations should engage in comprehensive ransomware protection. This includes the use of multi-factor authentication (MFA), firewalls, intrusion prevention systems (IPS), endpoint detection and response (EDR) systems and employee education. Just as important, if not more so, is backing up critical data to ensure seamless recovery after a ransomware attack.

***Candid Wüest, VP cyber protection research, Acronis:*** Detection and prevention are both important parts of defending against ransomware. As the ransomware operators continue to improve their platforms, it will become more important to focus on attack prevention, while not losing focus on detection of anything that might get past our initial defences. The harder it is to attack our systems, the less profitable it will be for cyber criminals, reducing their incentive to attack.

***Mark Raeburn, managing director at Context, part of Accenture Security:*** There is a certain inevitability to ransomware and none of us can afford to be complacent. But there are some practical steps we can take to improve the outcome. Properly test and test again. Many companies will believe they are well equipped to prevent ransomware but testing your defences is the best way to find out. Manage the problem and have a plan. For example, segregate the data that you care about, compartmentalise where you can and harden your network. These aren't new approaches, but it's important to get the basics right.

Being held to ransom is scary — I've known business leaders who have had physical threats of violence as well as the threat of releasing the stolen company data. But with the right preparation and testing, there's a much better chance of being able to maintain business continuity without paying the ransom.

***Raj Samani, chief scientist and McAfee fellow:*** Despite efforts to mitigate the risks, ransomware is not going away anytime soon. The tactic is too profitable and effective for cybercriminals. There are, however, ways to cut down the number of successful ransomware – or digital extortion – attacks. For example, organisations should follow basic cyber hygiene best practice. One of the key concepts to consider is that prevention is better than a cure. With this in mind, organisations should recognise what ransomware attackers are targeting and secure them before attacks occur.

Beyond simply detecting attacks, businesses can use technology that can learn from previous breaches to help prioritise threats, predict the types of campaigns that will be launched against them, and pre-emptively improve their defensive countermeasures. To support this approach, they should also build an open, flexible architecture that can adapt as needed without the need for bolt-on security.

In this way, they can achieve complete data and enterprise protection capabilities, underpinned by a holistic, proactive and open security architecture. Adopting a Zero Trust mindset can also help businesses to maintain control over access to the network and all instances within it, such as applications and data, and restrict them if necessary.

***Rory Duncan, GTM leader, security, NTT:*** Stopping ransomware is not simply a case of shifting from detection to prevention. In fact, for a business to become secure by design, both are equally important and should be executed as part of four, overarching steps: predict, prevent, detect and respond.

"Prevention is, of course, fundamental for ensuring that your organisation has done everything possible to prepare for ransomware threats. Importantly, paying a ransom will not guarantee that your data will be recovered, so creating a robust back-up strategy will help you recover most, if not all files, in the event of a ransomware attack. What's more, taking a Zero Trust approach to security is critical. The mass rise in remote working and distributed workforces over the last year has meant that businesses are struggling to define their network perimeters. In other words, traditional perimeter approaches to network security are not holding up and this has put organisations at a higher risk of being breached. By adopting the Zero Trust principle of "never trust, always verify" and implementing identity management and networking security controls and organisations can boost their network resiliency and address threats such as ransomware. Beyond this, introducing security awareness training should be a main component of every security programme, helping to reduce the risk of employees falling victim to ransomware via phishing emails, for example.

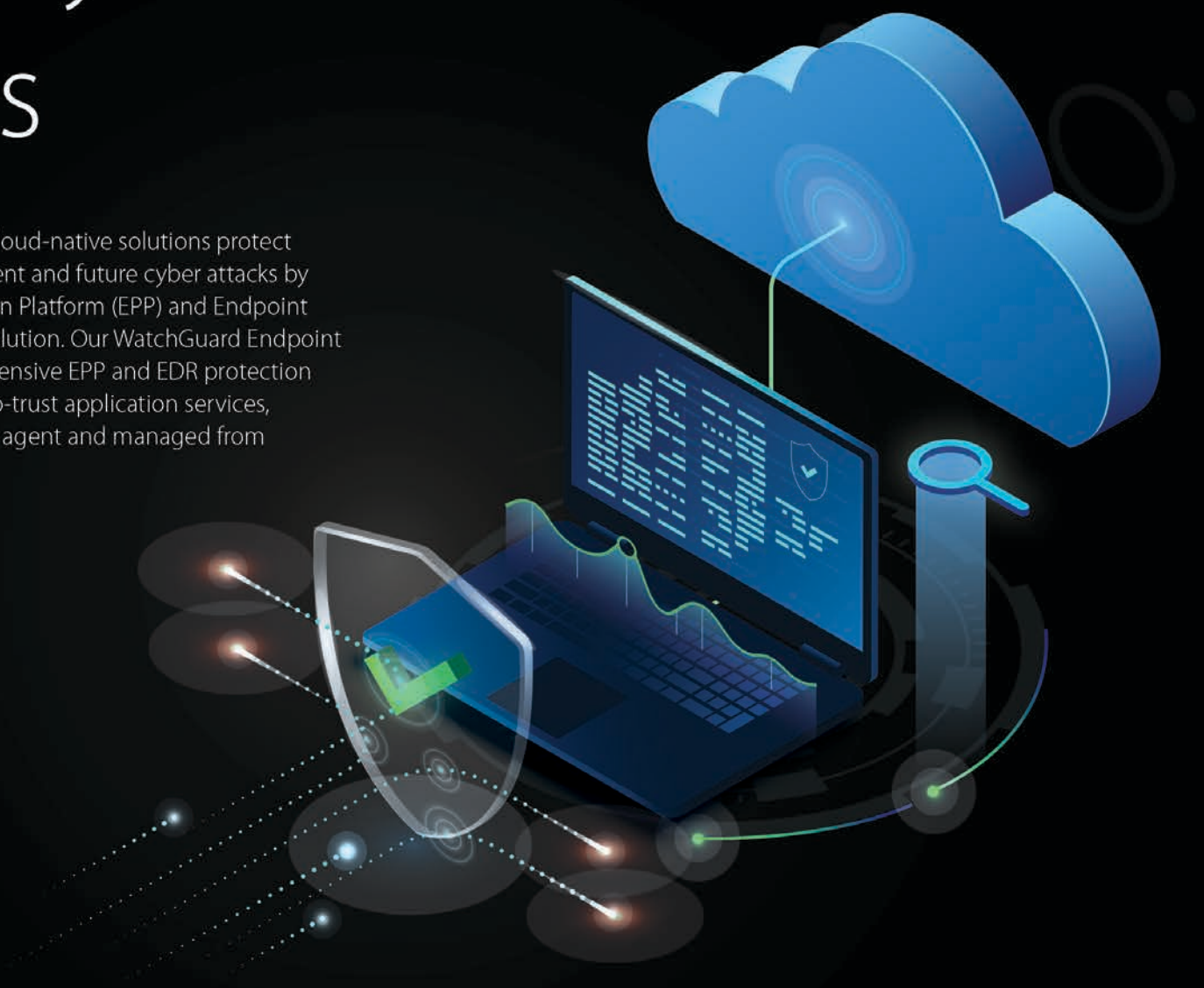
"Even with all of this in place, however, ransomware attacks are constantly evolving and cybercriminals are savvy, stopping at nothing to penetrate an organisation's defences. This is why having strong detection tools in place is equally as vital. Common detection methods such as anti-virus, IPS/IDS and sandboxing are all important for detecting known attack signatures. Meanwhile, new and unknown attacks require heuristics and anomaly-based detection such as behaviour modelling and machine learning. While these advanced, automated tools help organisations with huge volumes of data, human enrichment is still needed to pinpoint false positives and the needles in the haystack.

"Taking a holistic, Zero Trust approach to security is crucial in every industry. In sectors where IT and OT environments are becoming increasingly connected, having an all-encompassing view when securing IT and OT networks is particularly important. As demonstrated with the recent Colonial Pipeline attack, the potential for a ransomware attack on IT systems to cross over into an organisation's OT environment is a very real possibility. While it appears that Colonial was able to stop the spread of malware to the OT side, organisations should take this as lesson and apply the same monitoring and Zero Trust architectures to OT systems as they do IT environments. ■

WatchGuard Endpoint Security Solutions

# Confidently protect your devices

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



## WATCHGUARD EPP

**Endpoint Protection Platform**

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

## WATCHGUARD EDR

**Endpoint Detection and Response**

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

## WATCHGUARD EPDR

**Endpoint Protection Detection and Response**

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

Threat Hunting Service

Zero-Trust Application Service

+44 (0) 203 608 9070

uksales@watchguard.com

# The path to transforming control rooms operations with ESN and LTE communications

*Rhiannon Beeson, APD Communications & the British APCO executive committee*

As the UK ushers in a new era of LTE communications with their Emergency Services Network (ESN), Rhiannon Beeson of APD Communications and the British APCO executive committee shares her insights and advice for organisations upgrading to the ground-breaking technology.

"Technology is important, but we must always remember that it's a tool to improve public safety", says Rhiannon.

## In your experience working with control rooms, how are people feeling about ESN?

We know that the emergency services and organisations in the critical control field are excited by the promise of unprecedented access to data and new applications. The potential benefits are huge. However, in migrating to the technology, organisations are very aware of the scale of the project and the operational risks associated.

Their first priority is their continued commitment to public safety.

We've worked with our customers to create a 3-step approach. The first is 'Getting Ready For ESN'. This involves preparing your technology and suppliers, communicating and preparing your people and ensuring we understand the changes in processes too. The second phase is 'Business As Usual', continuing to save lives and serve the public is our top priority. And the final phase is 'Getting Value from ESN', which is where we discover new applications, access to data and a more connected public service.

Our collaborative and phased approach was so powerful, we created a webinar series and free resources to spread the word, they are completely free to download and available to everyone. They've really helped people embrace the change.

## You mentioned the 'Getting Ready For ESN' phase, what does this look like?

The UK currently uses the TETRA radio network for critical communication, location and a small amount of data. There are a large number of devices and applications that connect to this network to connect the whole organisation together.

The handheld radios are an example of the devices that need to be discontinued at some point, so organisations need to procure enough to last through the migration. Too many and they've wasted money. Too few and they cause a critical communication breakdown. So organisations need to assess their current stock, replacement rates and calculate how many they need. 'Handset pool partnerships' protect the public purse.

When you consider getting the control room ready, the first challenge is the almost-obsolete Motorola software called Centracom/Vortex, which only runs on Windows 7, an already obsolete Microsoft operating system. We highly recommend embracing the upgrades to 'Dispatch Communication Server' (DCS) and windows 10 ahead of any migration to ESN. This allows the replacement of complex analogue technology that occupies a large amount of space and power in server rooms and shifts towards modern IP-Based technology.

Inside the control room you have voice recorders, dispatch, maps, voice comms and location software and hardware. Organisations have to ensure their suppliers are prepared on time, otherwise they may need to run new procurement exercises.

But 'Getting Ready for ESN' isn't just about technology, current operational procedures and processes have to be considered. For example, if you have a mixture of LTE and TETRA handsets, do front line staff carry two handsets? Which one should they use? How does the control room know who to contact and on what network? How do they interact with each other in a major incident? Understanding these, and many more questions, helps to communicate and prepare the people involved in adopting and embracing the change, too.

## That sounds complex. What are you doing to help control rooms get to 'Business As Usual'?

I previously mentioned the webinars and free resources we've created that you can access via our website, but we are also working with suppliers like EE, Telent and Red Box to help everyone prepare for the change.

We've prepared detailed and tailored 'Ready For ESN' reports, including a high-level RAG (red, amber, green) status, highlighting what each organisation has completed and still needs to be done.

We've also created a full five-phase migration plan which recommends which teams should migrate first, when and why, along with a series of risk gates that you need to pass through to continue your roll out. It's pretty comprehensive and provides an idea as to how to manage the migration.

## As we get through the 'Business As Usual' phase, what do you think the future benefits will be from ESN and LTE technology for mission critical organisations?

The improvements in bandwidth to devices will open up a whole new world of possibilities. New applications will start to appear that provide front line teams with real time insights and information. Video streaming directly to the control room will become ubiquitous from body worn video, drones and vehicles.

We will start to see interactions between vehicles and devices such as aircraft, vehicles (V2X), IOT and drones to improve communication, situational awareness and public safety significantly. And we will see the technology being used to improve response times and reduce costs through the automated dispatch of drones instead of helicopters in certain circumstances.

The future of public safety and the emergency services looks bright through the adoption of industry leading LTE technology and the adoption of the ESN network is an exciting future for us all.

# Thinking outside the container

*Alex Chircop, CEO, StorageOS*

Cloud native computing and container-based platforms can deliver the solid reliability that developers and infrastructure managers require while enabling self-service, automated deployment and scalability. Developers and platform managers love them. Indeed, Independent research suggests that 95% of new applications are now developed within containers, with developers increasingly coalescing around Kubernetes. As a result, the demand for storage that supports cloud native workflows and stateful applications has never been greater. While compute, memory ,networking, and other orchestrator resources continue to mature, the evolution of persistent container-based storage seems to lag behind.

Until recently this had a profound effect on the adoption and growth of hybrid cloud environments with storage being a crucial layer for all stacks — data for stateful applications and services has to reside somewhere. The slow maturation of container-based storage means developers have historically struggled to take full advantage of Kubernetes, leaving their applications partially trapped in a world of legacy IT infrastructure.

People often ask me why storage has fallen so far behind. Frankly, it's because containerised compute, memory and networking were easier problems to address. It's human nature to deal with the easy stuff first and score some quick wins, however fixing containerised storage takes more time and effort. As a result, has been playing catch-up over the last few years.

## Speed and intelligence

Firstly, traditional storage approaches to support containerised environments such as SAN-based plugins — don't have the low I/O latency, throughput, bandwidth, or the intelligence to handle the rate of change and complexity needed to attach and detach volumes across clustered nodes. This is a reason why many developers don't move Kubernetes applications into production environments.

However, we're starting to see a new generation of high-performance cloud native storage solutions with enhanced local read performance capabilities, coupled with rapid failover, replication, in-memory cache, data reduction and built-in rules-engines. This directly contributes to the increased use of Kubernetes in production environments for mission-critical applications, including financial services solutions, trading platforms, managed service provider tools and telco services. No wonder, then, that recent Cloud Native Computing Foundation figures suggest 78% of cloud native projects now run Kubernetes in production.

## All applications need state

Next, containers are designed to allow applications to break the lock-in to a specific server or node and reduce infrastructure costs. For this to work to maximum effect, storage that supports container-based applications and platforms must provide the same portability, automation and orchestration capabilities as resources such as compute, memory and networking.

Finally, orchestrators like Kubernetes abstract IT infrastructure, providing a self-service platform with automated deployment, scaling, healing and connectivity. The key here is abstracted infrastructure. Storage infrastructure cannot be exempt from abstraction without negative impact on application development and deployment. It should not have any proprietary dependencies or be tied to any hardware, virtual machine, or cloud service provider. It should also be equally accessible on a developer's laptop, within an edge datacentre, and run without issue in cloud, on-premises or hybrid environments.

It's also apparent that organisations are not deploying one large Kubernetes cluster. They're deploying lots of smaller clusters and they need data (and therefore storage) to be accessible and consumable between them. This added another layer of complexity.

The solution is cloud native software-defined storage. It provides dynamically provisioned storage for cloud-native environments. It also gives developers the same composability and declarative function that they have with compute, memory and networking, plus the ability to extend that down to the storage level of their stack.

## How does cloud native storage work?

Once deployed, cloud native software-defined storage should have the capability to virtualise the storage resources in each node of the cluster — whether physical disks, VMs or cloud-based storage resources — and aggregate them into a single pool. As long as the disk or the underlying hardware is visible, it should be accessible.

Once you get to that stage, developers can dynamically provision storage volumes within Kubernetes just like compute, memory and networking resources. Data can appear anywhere in the cluster through a 'storage mesh' that spans each node. This means failovers can happen instantly as you dynamically expand or shrink the cluster and applications can continue to access their data wherever they are. Storage becomes predictable, reliable and most importantly, persistent.

While it's easy to write a manifesto for containerised storage, making it a reality is a different matter. One reason is that storage vendors are still focused on providing storage for Kubernetes linked to a server, an operating system or a hypervisor. They continue to build their solutions on proprietary hardware or software components as it's the only way they know how to ensure reliability and performance. Kubernetes is a new environment, with new rules and delivering storage for it to consume requires an entirely new approach.

# Age of interaction

## Ali Nicholl from Iotics looks at how digital twin technology can harness the power from vast amounts of data we gather at an astonishing rate

We live in an age where data is the transformative currency. Data is gathered at an astonishing rate and yet, according to Gartner, as much as ninety percent of it never gets used. So-called 'dark data' is the information gathered from digital assets about all aspects of activity and processes that ends up stored in the metaphorical cupboard under the stairs. Usually retained for compliance purposes only, this data is a security risk and a drain on resources, often costing more to store than the value it creates.

Data is only as useful as its ability to connect with other data to produce information that is greater than the sum of its parts. While many technologies simply act as data vacuums, digital twin technology harnesses data through interactions and its success is ultimately measured by the depth and span of its connections. It creates a network of data that provides valuable information about the world at large.

Within this information jigsaw puzzle, the digital twin can be seen as a piece of data that offers a way to describe other data. Data about other data is called metadata: it elaborates on what we already know and allows us to extract more information from the data we're examining. For example, a digital twin can illustrate key information such as how frequently data is being shared, where data is coming from, how it is being measured and what metrics are being used. Think of it this way: for centuries we have had windmills, and for most of that time all we really knew about them is where they were and what they did. It stands to reason that if you combine data on how much wind is being harvested, speed, volume, output, efficiency and downtime, you'll get more from your windmill.

*Data is only as useful as its ability to connect with other data to produce information that is greater than the sum of its parts*

Digital twinning helps to maximise these connections and while the more information a digital twin provides about the data at hand, the clearer the usefulness of the data becomes. It works in a similar way to writing an article based on open-source research. If you use only one on-line online resource that subsequently proves to be unreliable, then everything extrapolated from that source is unreliable. The more research sources you use, the more your chances of producing a reliable article increase. The odds become better still if you can establish the reliability of the source itself. Working on this principle, a digital twin is the scholarly article of a digital ecosystem. Each layer of data or information builds confidence in the value and competency of the data you're assessing.

What makes digital twin technology such a powerful tool for network and enterprise business managers is its ability to describe itself. The more data it provides, the more understood it becomes, which allows it to interoperate successfully within a network of other twins. This network creates a data mesh that allows a spectrum of data to communicate with each other, to be shared securely and ultimately output new data in an ongoing, adaptable and compounding data cycle.

We've talked about measuring the success of a digital twin and how it is only as strong as its connections to other data and, ultimately, its ability to describe that data. But empowered by connections and strengthened through detailed communication, digital twins can bridge the gaps between parts of an organisation where you wouldn't normally seek connections. With digital twin technology, everything is connected.

No enterprise does one thing only, but too often they operate as though they do. For example, a manufacturer will have a production line with systems for regulating the process. It might also have an onsite R&D team that's designing the item to be manufactured. These three functions will have their own set of systems and data set up to operate independently: and yet far more can be achieved if they are digitally interconnected. Digital twin technology can fill the gaps between functions and create a network between them, unlocking the full potential of data that works together as a federation. The three discrete data sources integrate into a web of sources that has the inbuilt semantics necessary to understand the three separate inputs.

The potential for collaboration is limitless as a digital twin follows the threads of a network that weaves its way through your business – customer base, supply chain, control systems. Everything has the potential to operate as one cohesive unit without needing to teach staff or systems how to be specialists in multiple areas. This is the value of digital twin technology: it interacts, making connections in places we didn't think connections could exist.

If this federation of twin technology is important in attributing value to your data, describing what's inside that network of twins can have an even greater effect by unlocking a digital supply chain of limitless potential. When you have access to both the data and the details of the data, you unlock the ability to make your own decisions on how to use it. You shouldn't have to jump through hoops to get the data you need, and neither should it end up in that 'data dump' of expensive unused junk. It should be accessible, tangible and put to work in a way that transforms the efficiency of your organisation. ■

# Design concerns for a micro data centre

*Vik Malyala, senior vice president, Supermicro*

As more computing moves to the edge and away from massive data centres, the need for a new type of data centre is becoming a critical piece of an edge to cloud strategy. Traditionally, large data centres have resided where there is a significant amount of space with easy access to low-cost power and multiple internet connections. However, new and smaller data centres that serve specific purposes are becoming a requirement for managing and filtering the vast amounts of data generated from 5G and IoT devices. By distributing the collection, analysis, and filtering of data closer to the edge of the network, new services can be created that respond quickly, reduce network traffic, and allow for more intelligent decisions.

Micro data centres that live closer to the physical location of data generation (for latency reduction purposes) can be designed and built quickly without significant corporate data centres or public cloud data centres. Because a micro data centre brings systems closer to its users – and the user closer to the server – latency may be lower than in a traditional data centre. This capability is one of the main reasons why companies are opting to move towards micro data centres and edge computing. Because, ultimately, the low latency aspect will help increase the speed of data processing, thereby boost efficiency and make many (highly complex) processes run faster and smoother.

To this end, there are a few items that need to be considered when designing and implementing a micro data centre.

1. **Find A Location** – A micro data centre needs to reside close to where the devices are located. Due to the limited range of Wi-Fi signals or other short range communication technology, locating the servers within a factory, store, or even at the base of a wireless cell tower is preferable. Micro data centres would typically be constructed from just a few servers, specifically chosen for a set of specific applications. Picking the right location for a micro data centre, which can perform assigned tasks, is critical for the uninterrupted performance of a small data centre.
2. **Understand the Environment** – Servers in a micro data centre may or may not look like traditional data centre servers. Rather than residing in a closely controlled environment (temperature, humidity, filtered air), these systems may need to withstand higher temperatures without additional cooling assistance. The servers may need to be "fanless," which means that the CPU heat dissipation is minimal and can cool itself. However, there may be restrictions on the ambient temperature where the servers are located. Therefore, it's crucial to understand the surroundings and conditions of where these servers are based and that the selected servers need to be sized to perform their function and work in the end environment. In addition, these servers will only need to draw as much power as can be delivered to their unique – often rather rural or remote – location and may not have redundant power available.

   In some cases, a single server will become a micro data centre and may be located outdoors or in a poorly ventilated closet. A telecommunications standard, NEBS (Network Equipment-Building System) Level 3, specifies several operating conditions that specific equipment must work within. Since these conditions are significantly more varied than for a large data centre, servers must be designed and tested under these conditions.
3. **Understand Connectivity** – Since a server in a micro data centre will most likely need to communicate upstream to larger data centres, it is essential to plan for and outfit the space with the wiring necessary for communication to other corporate systems. This may include the connections to the corporate network and possibly other facilities, whether inside a firewall or externally to the internet.
4. **Select the Right Form Factor** – As micro data centres may need to be placed in a confined space, the physical dimensions of the server may be quite different than in a more significant data centre. The measurements that a server may occupy are not standard. While, in general, a larger (physical) server can do more work, smaller servers are designed to perform specific tasks. They can use smaller form factors, as expandability may not be necessary.
5. **Reliability and efficiency** – Depending on the location of the micro data centre, servers need to be highly reliable, efficient, have long lifecycle support as IT staff, available power, access to systems for repairs, downtime, logistics etc can get quite cumbersome and expensive.

More micro data centres are appearing as greater amounts of data is being generated at the edge. There is a growing need to house servers in various form factors closer to where data is being generated, with the ability to perform analytics and filter the data before sending upstream to larger capacity systems. Although there are benefits and needs for massive scale data centres, this new reality of a distributed data centre will grow as more data is generated all the time, everywhere and by anyone.

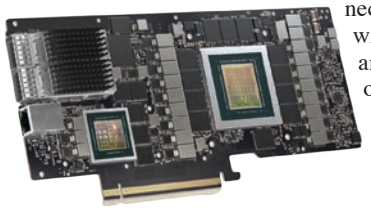
## PRODUCTS

Datwyler is a Swiss player, which boasts "creativity and drive, dependability and entrepreneurial spirit and a passion for shared success with our customers". The Datwyler Micro Data Centre (MDC) prides itself on being a compact, fully-preassembled plug-and-play IT infrastructure solution. It contains a 42U rack, among other things, an energy distribution unit, UPS, cooling unit, air gap sealing, an environment and security monitoring system as well as the associated sensors. Other key features include smart access control (key, card, keypad or biometric), backup batteries (MDC 200 / 300) an in-Rack cooling system, 3.6 kW (MDC 300) and sensors. There are optional extras, too. They include rack mounted fire suppression, a camera, cabling, emergency ventilation fans and an SMS alarm notification. In other words, the Datwyler Micro Data Centre is tailor-made and customised solution to fulfil the customers' specific needs and requirements. What's more, it can be deployed within a few hours. *datwylermdc.com*

Delta InfraSuite is a new generation, "highly-integrated modular data centre solution", the company says. It uses racks as the data centre carrier and fully integrates all sub-systems including UPSs, cooling, power distribution, lightning protection, fire control (optional), wiring, airflow management, intelligent monitoring, and more. Delta's modular data centre solution offers a data centre environment that provides safe equipment operations within the racks and supports the development and standardising of micro data centres that fit into racks. In addition, Delta InfraSuite takes up very little space, allowing quick deployment within a limited space, and it provides 10 types of solutions that require 20kVA power supply capabilities. Delta InfraSuite can be applied in micro data centres under 50 square meters or with an IT load under 20kVA. It is suitable for regional or small business environment IT applications. It terms of its "advantages", Delta cites the fact the Infrasuite supports the highest Class-A availability level, the fact it has highly-reliable emergency cooling and its "distributed control increases reliability".. *deltapowersolutions.com*

Kstar says its IDU micro data centre is a new generation of alternative solution to small IT room, with complete integration of a "dynamic environment monitoring system, power supply, distribution systems, battery, cooling system, cabinets and containment and the hot aisles and cold aisles are isolated to lower PUE to 1.3." It is designed to meet the IT room infrastructure optimisation needs and mainly used in small- and medium-sized enterprises, microenterprises, large enterprises, governments and other branches in finance, education and energy industries. Kstar reckons "the forward-looking enterprises have realised that the intelligent single-Cabinet IT room (micro data centre) with high reliability and availability is the future trend" from the perspectives of both current short-term investment and future long-term operating costs. The micro data centre can be used in the application that the cabinet is within 10 and total load is less than 40kVA. Other key features are quick deployment and the fact it's energy-efficient. n*kstar.com*

The Nvidia BlueField -2 data processing unit (DPU) is the world's first data centre infrastructure-on-a-chip optimized for traditional enterprises' modern cloud workloads and high-performance computing. It delivers a broad set of accelerated software-defined networking, storage, security, and management services with the ability to offload, accelerate and isolate data centre infrastructure. With its 200Gb/s Ethernet or InfiniBand connectivity, the BlueField-2 DPU enables organizations to transform their IT infrastructures into state-of-the-art data centres that are accelerated, fully programmable and armed with "zero trust" security to prevent data breaches and cyber-attacks. By combining the industry-leading Nvidia ConnectX -6 Dx network adapter with an array of Arm cores and infrastructure-specific offloads, BlueField-2 offers purpose-built, hardware-acceleration engines with full software programmability. Sitting at the edge of every server, BlueField-2 empowers agile, secured, and high-performance cloud and artificial intelligence (AI) workloads, all while reducing the total cost of ownership and increasing data centre efficiency. The Nvidia DOCA™ software framework enables developers to rapidly create applications and services for the BlueField-2 DPU. Nvidia DOCA makes it easy to leverage DPU hardware accelerators, providing breakthrough data centre performance, efficiency, and security. *nvidia.com*



Edge and the micro data centre have become essential elements in the expanding data network that is the platform for our data economy. Gains in processor performance and the need for location specific compute for the myriad applications that require ultra-low latency communication, means that features that were based in traditional data centres are now deployed where the user and the data source reside. The micro data centre is a means for processing Edge data, which may be gathered from vehicles, traffic automation systems, surveillance devices, local 5G networks, office and factory facilities. The data must be gathered and processed locally to improve the performance of the overall system. As the volume of data increases so does the need for micro data centres' performance to rise to utilise the AI and ML-based applications required to process, analyse and respond to the data. Today's micro data centres are standalone systems such as the Ku:l Micro Data Centre, offering highly configurable and scalable solutions to enable accelerated corporate applications, HPC (high performance computing) and AI workloads in any Edge environment whilst maintaining data centre density. These micro data centres can be as small as a filing cabinet and scale up to 48U rack cabinets and are often usually configured for specific workloads to maximise efficiency. As standalone systems they contain features typical in traditional data centres: CPU and GPUs, a cooling system, storage, security and reserve power source. Iceotope's Ku:l Micro Data Centre utilises Lenovo's ThinkSystem SR670 2u rack server and delivers HPC performance supported by four GPUs per server. Integrating the server into a liquid cooled chassis eliminates the need for any air cooling, delivering an almost silent, energy efficient solution with >95% heat capture and rejection via a heat rejection unit (HRU) and the sealed chassis removes the need for humidity monitoring. *iceotope.com*

# Please meet...

*Alexander Schebler, co-founder and VP carrier relations, EMnify*

## What was your big career break?

The most significant milestone in my career to date was founding EMnify, together with Frank Stoecker and Martin Giess. When I think back to that decision, we didn't even consider it a decision – we were compelled to start the company based on what we had collectively seen in our telecom's careers so far. We recognized early that connectivity would have to become a cloud-native resource. So, we set out to ensure that it did, completely disrupting the telecoms market.

## Who was your hero when you were growing up?

I always looked up to my dad and continue to, today. He's not at all into computers and technology! He is a true craftsman – he skillfully and thoughtfully applies his mind and his hands to every project or task – whether creating something from scratch, improving it, repairing it, however big or small. We have even built houses together. I really admire his focus, diligence and commitment to his craft – he gives it everything but still manages to be there for his family.

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

This is tricky. I honestly haven't ever given it much thought. I know I'm right where I should be. But if I had to choose… On a personal level, I'm a car fan and so I do take an interest in the automotive industry. But on a professional level, I need quick feedback loops, fast growth, disruption – visible positive change every day! I think I'm too impatient to work in the automotive industry.

## What would you do with £1m?

Invest it in EMnify! We recently celebrated our 7th anniversary. It's incredible what we've done in that time: completely transform a complex cellular connectivity into an easy to consume cloud offering, build the largest GSM footprint that a non-MNO company ever built - covering 185 countries with 350+ direct roaming agreements (and still growing). Just last week, we launched LTE-M service in 45 countries.

We've grown the team to 112 global IoT experts who serve almost 2000 customers – enabling groundbreaking IoT solutions worldwide. And, we have only just begun! But you never know what opportunities the ecosystem of tomorrow will bring – so it always helps to be ready to jump on them.

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

It's a mixture of things but it all comes down to taking a breath before reacting – to anything, in work or in life. Yes, we all want to make decisions quickly. But every decision should be given the time and consideration it needs. Don't send that reactive e-mail at the end of the day, if you don't have to – sleep on it. Always sleep on it. We are at our best when we are calm and have given things due consideration. People will appreciate a considered response more than a rushed one.

## If you could live anywhere in the world, where would it be?

I love travelling and have been very fortunate to be able to travel a lot in my life – in Africa and Asia, for example. I have a huge appreciation for southeast Asia. I love Hong Kong: the vibrancy and energy and people! But when it comes to living in a place – ideally it should be calm, quiet, safe since I'm not just thinking of myself but of my family. That said – being close to an airport is always a bonus!

## What's the best thing about your job and industry?

The global aspect of what we do and the interaction with customers and suppliers on a truly global scale - different cultures and languages come with different expectations and interactions. It can be challenging, at times, but most of the time it's incredibly enriching. A very concrete example to bring to life what I mean: EMnify's first customer was in Australia. A German start-up with its first customer in Australia? We didn't know borders from day one.

## What will you do when you retire?

I have no idea. I don't give it much thought. I think if you're thinking a lot about retirement at my age then you're longing for an escape, but I can happily confirm this isn't the case!

## What's the most valuable lesson you've learned?

It's no secret that starting a company brings with it many pressures – both inside and outside of the actual job. There are two important lessons I learned the hard way in the early days of EMnify's founding – 1) learn to say no, and 2) you can't please everyone. As much as you want to make a decision that guarantees the best outcome for everyone involved – this is hardly ever possible. Trying to please everyone usually ends up upsetting everyone!