

## Public & private blockchains

The differences explained

Jonas Lundqvist,  
Haidrun, p7



## Critical comms and 5G

How will 5G help the emergency services?

Jason Johur,  
TCCA, p15



## Top tips from an expert

What you need to know about IoT security

Keith Glancey,  
Infoblox, p15



# Budget 2021: NHS gets £2.1bn IT cash injection



**Chancellor of the exchequer Rishi Sunak ringfenced £2.1bn in this year's budget, which he said will go toward improving IT and technology in NHS hospitals across the country.**

The cash injection covers the introduction of digital systems for healthcare organisations that have not previously used them, restocking and updating antiquated technology, improving cybersecurity and expanding the use of shared digital care records.

This extra investment in IT and data services to create digital patient records is part of the government's larger £5.9bn capital funding to help the NHS clear the record backlog of patients waiting for treatment.

In addition, there will be support for around 100 "one-stop-shop" community diagnostic centres across England, to assist those waiting for clinical tests such as MRIs, ultrasounds and CT scans.

One in 10 trusts still operate on "paper-based systems" according to health and social care secretary, Sajid Javid. NHS trusts have been seeking an additional £1.8bn per year by 2024, which would take the overall NHS capital budget to £10.3bn.

Figures released earlier this month showed GPs were also facing record demand with 24 million appointments taking place – above pre-pandemic levels.

Greater use of technology has meant that a reported 1.25 million text messages and 300,000 emails were sent to parents of toddlers, informing them of booking appointments for Covid jab for their children.

The £2.1bn to improve efficiency and security in the NHS is part of a larger £5.9bn capital funding to help the NHS clear the record high backlog of patients waiting for treatment.

Furthermore, the IT investment has been well-received by the UK's technology sector.

Mike Kiersey, chief technology officer at Boomi, the integration platform as a service (iPaaS) company, told *Networking+* how the UK public sector has been reliant on a multitude of disconnected legacy IT systems for decades "and it is clear that these current systems" cannot meet today's clinical needs. "Long-awaited, the sweeping shift towards digital transformation brought on by Covid-19, has led Sunak to set aside £2.1bn to fund the modernisation of NHS IT," he said. "The UK's public health service

runs on the efficiency of information and accuracy and recency. If, as the report notes, some of the data and technology infrastructures have been unable to keep up with rapid changes, then that is a serious concern, especially given current circumstances where data needs to be consistently managed, integrated, secure and accessible to best serve the public."

Kiersey added that funding being directed to future proof IT systems is promising, "but digital transformation is still a delicate process and one that needs to be carried out over a long period of time". He said: "If the NHS can successfully modernise its data practices in the coming months, it will be able to put a framework in place and become a digitally native system that can start addressing the backlog of people waiting for crucial checks, tests and scans and to help reduce waiting lists. Overall, this will ensure digital systems in hospitals and mental health care settings are entirely robust, connected and efficient."

Prior to the budget, the Chancellor explained how the government is "committed to getting health services back on track" and ensuring no one is left waiting for vital tests or treatment". ■

**MobileMark**  
antenna solutions

**Innovative Antenna Designs  
Responsive Manufacturing  
Trusted Partner**

## 'Only two-fifths of UK IT leaders able to respond to cyber incident today'

Well under half (39%) of UK businesses feel confident in their ability to respond to incidents today, according to new research from Rackspace Technology.

Evolving security threats and attack methods, increasing attack opportunities as data volumes, digital operations and remote work continue to grow, are cited by 60% of IT leaders as the greatest cybersecurity challenges they face.

In addition, 53% of IT decision makers do not have the capability today to identify security incidents across multicloud environments. When it comes to mitigating threats, only 38% of those surveyed feel confident in addressing them today, while only 36% feel assured in addressing regulatory compliance.

In relation to data, just two in five (41%) are currently confident in their ability to protect critical data and warehouses, with a further 45% believing they will reach that point in the next three years. When it comes to assessing cybersecurity capabilities and needs on a periodic basis, only two in five (42%) felt comfortable in this area.

Moreover, almost half (44%) of companies are finding it hard to retain and recruit cybersecurity talent, though a similar proportion (45%) are confident in their internal initiatives in terms of cybersecurity talent retention.

The cybersecurity skills touted as the most important were cloud security (42%) and data privacy and security (40%). Despite its importance, a third (32%) of companies believe the biggest cybersecurity skills gap is in relation to cloud security.

With regards to staffing and skills concerns, over half of UK businesses (55%) rely on in-house staff with some external third-party help. A similar number (56%) said they use up to five external partners to provide cybersecurity. When looking into the types of cybersecurity partner the businesses engage with, the most sought-after are security value added resellers (47%), managed security service providers (45%) and managed detection and response providers (41%). Meanwhile, the top three areas of cybersecurity most likely to be handled by external partners are around integrated risk (44%), application security (44%) and data security (37%).

"Cybersecurity is one of the most important digital elements for UK businesses, but also the trickiest to address," said Andy Brierley, UK general manager at Rackspace Technology. "This is particularly true due to the accelerated pace of digital transformation across key sectors."

When asked about their companies' overall cloud security, 35% said they were at intermediate level, having to rely on third-party tools. An additional 32% described themselves as cloud-centric, meaning they use native tooling mixed with third-party tooling. ■

## ITAD firm opens three new sites

N2S, business which recycles IT equipment, has announced further expansion with new sites in Berkshire and Nottinghamshire as well as extending its Bury St Edmunds facility.

The new Reading site of approximately 13,500 sq ft, opening in mid-October, "will be a centre of excellence for the refurbishment and resale of pre-used IT equipment". These include servers, PCs, laptops and mobiles, with an immediate staffing of 15 experienced technicians, sales personnel and administrators.

Huthwaite near Mansfield will see N2S opening a 50,000 sq. ft facility in early November. The company will transfer 20 staff from the current Mansfield distribution centre operation and up to another 30 by Easter 2022. This additional site will be a

recycling and recovery facility for IT and telecoms equipment.

N2S is also expanding its Suffolk-based facility by 10,000 sq. ft to cope with the increase in volume.

"E-waste continues to be a growing challenge," said Andy Gomarsall, chairman of N2S. "Our aim is to increase the overall recovery rates in the UK market which have been going backwards in the last few years. Our new facilities will bring the extra capacity we need now and in the foreseeable future to support continued demand from customers for the recovery, refurbishment and resale of pre-existing IT products. Additionally, for processing equipment beyond repair prior to it undergoing N2S' patented bioleaching refining and recycling process at our main facility in Bury St Edmunds."



N2S recently announced a significant recruitment drive to fill more than 100 new job vacancies anticipated over the next 12 months. This has followed rapidly increasing demand from large UK businesses, government departments and local authorities for the company's highly sustainable ITAD and technology lifecycle solutions. ■

## Medieval Sherwood Forest gets 5G upgrade

A data-collecting robot dog, internet-controlled drones and a 5G upgrade are among technology being trialled by Nottinghamshire County Council to enhance the visitor experience at Sherwood Forest.

Birmingham City University has provided the site with the robot dog, which will collect data and upload it via the 5G connection.

If the trial is successful, the dog will gather data from areas that are usually inaccessible to help monitor and assess the health and condition of the forest environment.

The authority said the £10m investment would make it the world's first 5G-connected

forest and hopes to offer visitors an augmented reality headset to view an immersive Robin Hood-themed film.

The trial also covers the area around the forest, including Rufford Abbey and has been part-funded by the government's Rural Connected programme. Moreover, it is also hoped the 5G technology will help businesses in the area.

Councillor Keith Girling said the 25-month project had the potential to attract "millions" of pounds of tourism trade.

"It's going to draw attention to Nottinghamshire, which has got to be a good thing for investment," he said.

The forest will also feature what is



claimed to be the world's first interactive holographic film called An Arrow In Time. Using augmented reality headsets, the production features well-known characters from the legend of Robin Hood. ■

## Australian firm secures 40% stake in DC firm Kao Data

Australian infrastructure group Infratil has committed some £130m to Kao Data in London, with plans to expand its portfolio to £500m in the medium term.

Under the terms of the deal, the antipodean firm will obtain a 40% stake in the UK data centre business with current owners Legal & General and Kao Data founder Goldacre retaining a 30% stake each in the firm.

Jason Boyes, Infratil's chief executive officer (CEO), said his company's capital would initially fund the construction of a second Kao data centre at the company's Harlow campus. It will also pay for the acquisition of two other data centres, located close to Harlow, from a major UK financial services group.

Furthermore, Boyes added that with plans to build two more data centres at the Kao Harlow campus, it would bring the portfolio in the medium term to six, offering a total of 55MW capacity catering to a highly-specialised area of high-performance computing.

"Clearly, both L&G and Goldacre have the financial firepower between them to develop Kao to any scale they want, but what they have both been looking for is a partner with deep hands-on, scaling and building data centre business, experience," he said.

Lee Myall, CEO of Kao Data, added: "This investment presents a strategic opportunity to accelerate our mission of supporting the computing requirements of advanced industries, and to do so sustainably." ■

## Echelon to build second UK facility

Irish-owned Echelon Data Centres has inked a £182m deal with an affiliate of Starwood Capital Group to jointly buy and construct its second UK data centre, LCY20.

Based in Chesham in Buckinghamshire, the site will have a capacity of 30MW and it joins Echelon's LCY10 site, a 20MW facility in London's Docklands.

The Irish firm said that power is already fully installed on the LCY20 site meaning the data centre capacity can be delivered by late 2022, ahead of most other London area data centres.

Echelon, which now has six sites across Ireland and the UK with a total potential capacity of up to 500MW, believes that all data centre infrastructure should be powered by 100% renewable energy.

However, the company said it recognises that, in the short to medium term, hybrid solutions (such as on-site gas-fired peaking plants) may be necessary to support over-burdened grid infrastructure and to assist the transition to a wholly renewably-supplied grid system. ■

## CGI signs 'smart' deal with Edinburgh Council

IT and business consulting firm CGI has signed a five-year deal with Edinburgh Council to transform the capital into "one of the world's leading smart cities".

Included in this deal is the deployment of the CGI SensorInsights360 technology, which provides data insights, processes and tools required to deliver services.

"Edinburgh has big ambitions in becoming a world-leading smart city – a digitally inclusive and sustainable city with services that are easily accessible by

all of our residents no matter where they are in the city, or what their circumstances are," said City of Edinburgh Council deputy leader Cammy Day.

CGI SensorInsights360 – which will be implemented through a Smart City Operations Centre – provides an end-to-end approach to the Internet of Things (IoT), asset data collection and asset management, helping to identifying ways to improve efficiency and manage critical services in the Scottish capital. ■

### EDITORIAL:

Editor: Robert Shepherd  
roberts@kadiumpublishing.com

Designer: Ian Curtis

Sub-editor: Gerry Moynihan

Contributors: Iain Davidson, Ron Davidson, Jason Johur, Russ Kennedy, Tim Mercer, Corey Nachreiner, Mark Richman, Peter Ruffley and Tina Yates

### 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

© 2021 Kadium Ltd. All rights reserved. The contents of the magazine may not be reproduced in part or whole, or stored in electronic form, without the prior written consent of the publisher. The views expressed in this magazine are not necessarily those shared by the editor or the publisher.

ISSN: 2052-7373



## Amazon pens deal with UK spy agencies to host top-secret data

The UK's three spy agencies have contracted Amazon's cloud service unit AWS to host classified material in a deal designed to boost the use of artificial intelligence for espionage.

According to a report in the *Financial Times*, spy agency GCHQ championed the procurement of a high-security cloud system and it will be used by sister services MI5 and MI6, as well as other government departments such as the Ministry of Defence during joint operations.

The deal was agreed earlier this year and the data will be in Britain. GCHQ and AWS have so far declined to comment on the report.

In February, Britain's cyber spies at GCHQ said they had fully embraced artificial intelligence to uncover patterns in vast amounts of global data to counter hostile disinformation and snare child abusers.

The agency has been using basic forms of AI such as translation technology for years but is now stepping up its use, partly in response to the use of AI by hostile states and partly due to the data explosion that makes it effective.

GCHQ director Jeremy Fleming told a conference the number of ransomware attacks had doubled across the UK in 2021, compared with last year.

Meanwhile, AWS is offering UK councils a three-month crash course in cloud computing at zero cost. The program for local councils and government authorities, which includes both consulting services and infrastructure and software solutions from AWS, also comes without the need for contracts.

The program will be run by the AWS government transformation team and during the three months, UKs councils will see the creation and testing of proof of concepts (PoCs), through which they'll be able to see the benefits of digital transformation.

AWS will demonstrate how cloud can be leveraged to simplify payment management, reduce contact centre queries, clear data entry backlogs and information requests. It also says cloud "eliminates bottlenecks" and addresses underlying problems to issues such as data silos and skills shortages. ■



## Cumbria Police embraces 'TETRA radio refresh'

Cumbria Police has deployed a new range of Sepura SC21 hand portable radios to its police officer roles and SCG22 mobile radios in its vehicles as part of a "TETRA radio refresh".

The transition to the SC21 and SCG22 devices began with a trial undertaken during the Covid-19 pandemic in the UK and saw Sepura use a 'provisioning service', meaning the radios were pre-programmed and delivered to force headquarters ready to deploy as part of a "safe and accelerated transition".

ICT operational change business lead at Cumbria Police, Adrian Johnson, said the SC21 radios offered an upgrade on the force's previous devices due to their "powerful TETRA engine" and ability

to maintain Airwave coverage in the county's vast rural areas. The SCG22 mobile radio was purchased at the same time as it has comprehensive deployment options, including car, van, motorcycle and desk mount options, and shares a common interface to the SC21 acting as "a gateway".

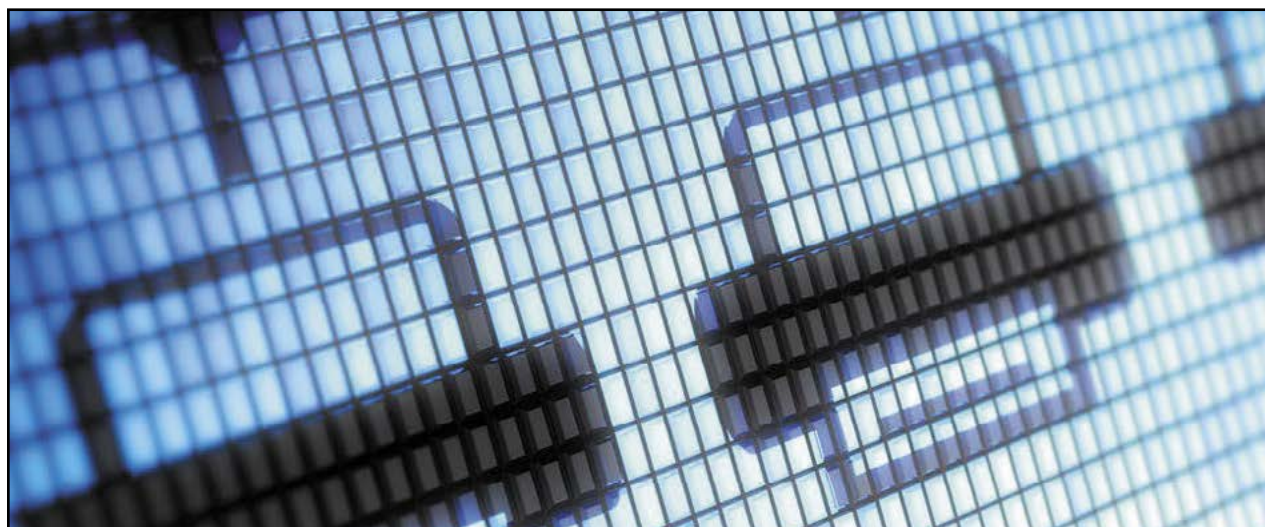
The radios were also programmed with a bespoke user interface which offered Cumbrian officers "a familiar user experience" to minimise officer training.

"Our officers have been providing policing services to our citizens and visitors to Cumbria throughout the Covid pandemic," Johnson said. "The Sepura rollout occurred during this global pandemic, during which the team had to

learn new ways of doing things safely.

He added that it is imperative in a mission critical environment that Cumbria Police has excellent relationships with suppliers and immediate access to subject matter experts when technicians need help or advice.

More than 1,400 new Sepura radios have been deployed across the county as part of the "refresh". ■



### printserver ONE - the optimised Print Server for a secure network

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

#### Your Benefits

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



printserver ONE

**NEW**



#### For All Printing Systems That Feature a USB Port

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



**SEH - 35 years of innovative product development**

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

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

Made in Germany



# Moving wireless forward

Mobile Mark is a leading supplier of innovative, high performance antennas to wireless companies across the globe. We've been in the wireless industry for over 30 years and have our roots in the early Cellular trials. We have grown and evolved over the years, along with the industry. Today, we benefit from enhanced design capabilities and expanded production capacity – along with a greater understanding of new and emerging markets – all of which have allowed us to become one of the best antenna developers in our field. Our customers have been our partners throughout the years. We believe in taking the time to understand our customers' individual needs. Through close consultation with clients, we are able to deliver innovative, tailored solutions that meet specific antenna requirements. Rapid prototyping capabilities allow us to take our designs from concept to reality in an extremely short time span, and to verify the performance of the antenna. A variety of network analyzers and an anechoic chamber enable us to conduct measurements up to 13 GHz, and ensure that the antennas designed meet or exceed customer requirements. We have onsite injection molding equipment and a fully equipped modeling shop staffed with skilled model makers to assist in the design phase and help us come up with a superior product – an antenna that not only meets the customer's electrical specifications, but is also very attractively packaged. Mobile Mark antennas are used in many sectors of the wireless industry. Here are just a few examples:

- Emergency services
- Commercial fleet management
- Public transport & bus management
- Smart cities & smart highways
- Remote monitoring & surveillance
- Mining & exploration
- Asset tracking & RFID

Let us know how we can help.

We understand the RF wireless world and are ready to help you evaluate your options. Contact us by email, phone or fax and let us know how we can help.

Mobile Mark Europe Ltd  
8 Miras Business Park, Keys Park Rd.  
Hednesford, Staffs.  
WS12 2FS, United Kingdom  
enquiries@mobilemarkeurope.co.uk  
www.mobilemark.com  
Tel: (+44) 1543 459 555  
Fax: (+44) 1543 459 545



## 'Remote workers pose greater security risk than office workers'

A survey of UK cyber security, IT and business professionals commissioned by WatchGuard Technologies, 75% of respondents believe that remote workers pose a greater IT security risk to their business than office workers. This heightened level of threat as most companies return to a mix of home and office working post pandemic, contributes to the massive 83%

of respondents who feel that cyberattacks on their business will increase over the next 12 months. When it comes to identifying specific threats, phishing attacks are still at the top of the list, followed closely by ransomware. Over half of the organisations polled said that they had experienced an end-point attack targeted at end-user computers and mobile devices over the last 12 months.

## Full fibre broadband for Uttoxeter businesses

Fibre-to-the-premises provider LilaConnect has started construction of a new full fibre network in Uttoxeter to provide businesses "with fast, stable, and secure internet connectivity". It is expected that the first premises will be able to connect to this new gigabit full fibre network in early 2022, with all businesses across the town having access by the end of 2022. "Accelerated by the global pandemic, a fast and reliable broadband connection has shifted from being a luxury to an

essential utility," said Brett Shepherd, managing director at LilaConnect. But it's much more than just streaming video and music or online shopping, it's also about transforming communities with improvements such as better access to employment, education, and healthcare. Having an open access full fibre network will future-proof Uttoxeter's digital infrastructure and provide the reliability and bandwidth that is invaluable to residents and businesses in the town."

## Cambridge University stops £400m deal with UAE over Pegasus spyware claims

The University of Cambridge has called off talks with the United Arab Emirates (UAE) over a record £400m collaboration after claims about the Gulf state's use of controversial Pegasus hacking software. A report in the Guardian said the proposed deal, initially hailed by institution as a "potential strategic partnership ... helping to solve some of the greatest challenges facing our planet" – would have included

the largest donation of its kind in the university's history, spanning a decade and involving direct investment from the UAE of more than £310m. However, Stephen Toope, the university's outgoing vice-chancellor, said in an interview that no meetings or conversations with UAE were now taking place after revelations related to Pegasus, software that can hack into and secretly take control of a mobile phone.

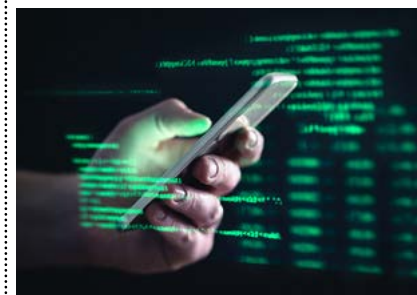
## CityFibre donates to community interest group

CityFibre has teamed up with Leeds community interest group, Geeks Room CiC, to provide equipment, including laptops and monitors, to support a new programme helping older students gain employment. The group provides an alternative environment to the traditional school, with children (aged 8-18) given the opportunity to learn through gaming (known as Game Education) and practical lessons. Its inclusive approach is intended to pull down barriers and ensure children with differing abilities and needs feel valued, connected to others and able to make positive contributions to the group

and wider community. The team's inclusive centre is host to a range of courses, including coding clubs, technical classes and design workshops. "Technology donations play an essential role in this and we are grateful for CityFibre's support as we expand our offering even further to help students gain employment," said Becky Wetherill, head of management and communication at Geeks Room CiC. The partnership with CityFibre has enabled them to expand the programme, including additional support for older students (aged 16-25) to help develop employability, educational, social and life skills.

## 'Dark Web is more dangerous than ever'

Stolen data spreads 11 times faster on the dark web today than it did six years ago, a new study has found. Conducted by cybersecurity vendor Bitglass, the report concludes that the dark web, the part of the World Wide Web only accessible by means of special software, has become darker, busier, and more widespread than ever before. Bitglass reached this conclusion by recreating an experiment carried out in 2015 and comparing the results. Researchers listed links to fake files with supposedly stolen credentials on various dark web marketplaces. These boobytrapped files helped the researchers keep tabs on the files as they circulated on the dark web, gathering valuable insight into the dynamics of the underground marketplace.



## British spies 'ready to hack'

British spies are prepared to carry out cyberhacking to bring down criminal gangs behind damaging ransomware attacks, the director of GCHQ has warned. Jeremy Fleming said the new National Cyber Force, a joint initiative between GCHQ, the military and MI6, could "go after" the cyber gangs, many of which are thought to be abetted by Russia and China. It is understood that these operations could involve carrying out counter-hacks of the gangs and forcing them offline. However, Fleming said the priority was for UK businesses to mount a better defence to ransomware hacking operations as basic cybersecurity prevented most harm and "it's not rocket science".



## Swansea 'lagoon' to house new data centre

An international consortium led by Welsh company DST Innovations is behind plans to build a £1.7bn renewable energy project on Swansea's waterfront, which includes a data centre run on renewable energy. The proposed Blue Eden tidal lagoon will house what is said to be the UK's first data centre powered by an uninterruptable source of renewable energy. The heat generated by the computer servers in the centre would then heat 5,000 new eco-homes along the waterfront. Blue Eden would be developed in three phases over twelve years, starting in 2023 with 1,000 jobs making high tech batteries for energy storage.

## Word on the web...

### Keep the gremlins out of your data

By Florian Malecki, vice president international marketing at Arcserve

To read this and other opinions from industry luminaries, visit [www.networkingplus.co.uk](http://www.networkingplus.co.uk)





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

# *Smart. Autonomous. Always moving.*

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



Works peer-to-peer to maintain **hundreds of connections simultaneously** for 'never break' mobility



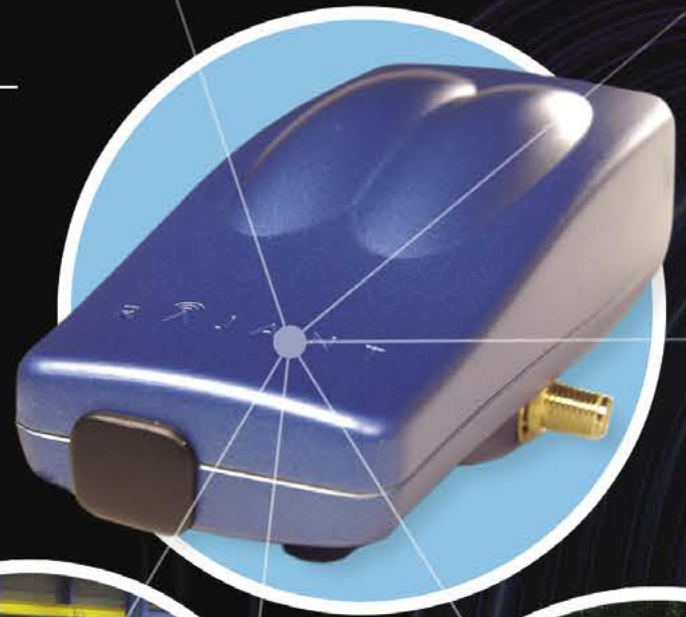
Intelligently self-optimizes to **change in real-time**, ensuring mission-critical reliability



The *only* network to enable **machine-to-machine communications** required for autonomy



Provides **Industrial Wi-Fi** for **extended Wi-Fi connections** in challenging environments



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

Industrial Wireless Networks **Unleashed.**



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

 **RAJANT**



# How threat actors use small security holes to infiltrate enterprise networks



**Combatting the rise of malware-as-a-service, by Ron Davidson, VP R&D and CTO at Skybox Security**

**M**alware-as-a-service (MaaS) has grown into a massive revenue stream for cybercriminals. This SaaS-inspired business model for hackers typically targets large enterprises with critical or sensitive assets. Now, the attacks are accelerating, thanks to MaaS's power and ease of use.

Experienced malware creators have developed MaaS platforms to sell incredibly disruptive capabilities to a new tier of potential threat actors: Wannabe cybercriminals whose lack of exploit-writing skills previously limited their ability to actually damage victims. While MaaS is similar in concept to traditional software as a service (SaaS), it's designed as a turnkey solution for non-technical cybercriminals offering paid access to malware-spreading botnets, web-based attack-monitoring tools, and even technical support. Armed with MaaS, low-level hackers can hold companies to ransom, while MaaS vendors profit just by offering the tools.

## Is "medium-severity" a false sense of security?

MaaS normally targets under-protected and easy to infiltrate "low- to medium-severity" vulnerabilities. Organisations relying on legacy remediation techniques and the Common Vulnerability Scoring System (CVSS) will prioritise addressing "high-severity" vulnerabilities first. However, the severity is not the only factor that impacts risk levels – a fact threat actors now exploit by using seemingly small security holes to open larger doors into networks.

Focusing on high-severity issues too often leads security teams to ignore medium-severity vulnerabilities, which commonly remain unpatched for extended lengths of time. Even though they account for a remarkable 41% of total vulnerabilities globally. With so many potential network weaknesses exposed, MaaS attackers have realised they can stop targeting the obvious issues security teams regularly patch (instead of leveraging "less severe" vulnerabilities as a way to penetrate networks).

Based on the number of new malware samples identified in 2020, it's obvious that COVID-19 fuelled the tenacity of cybercriminals: Ransomware samples increased by 106% year-over-year, and trojans surged 128% during the same period. Moreover, numerous incidents have demonstrated that MaaS has morphed into a profitable and sustainable asset for both cybercrime gangs and hostile nation-states. MaaS was previously linked to novice attackers, but the North Korean Lazarus Group's recent use of Trickbot's MaaS revealed that even experienced practitioners benefit from this technology to carry out attacks.

## Illuminating a new path forward for breach prevention

Security teams can arm themselves against potential invasions by addressing medium-risk vulnerabilities. The first step: Focus on breach prevention, which can be achieved in three ways.

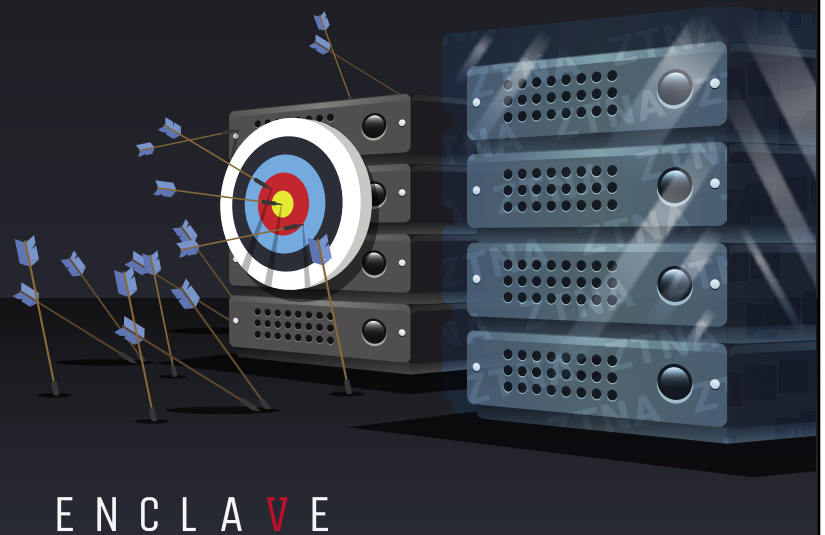
- **Obtain attack surface visibility:** A security team must first achieve comprehensive visibility of the entire network; this is the only way to know exactly what needs to be protected. Without accurate visibility, a security programme will always be only partial, missing potentially important context. A complete overview is critical to mitigating risks across traditional and hybrid networks spanning physical, virtual, and multi-cloud assets.
- **Use simulations to predict the next attack:** Today's technology enables potential attacks to be simulated before they occur using an offline, contextually aware model of the network and its security controls. Having access to a full, detailed representation of the attack surface enables security teams to search for vulnerabilities in highly complicated environments. Zeroing in on exploitable and exposed vulnerabilities will help enterprises understand how to patch and protect the flaws in their networks.
- **Aggregate disparate data for full visibility:** According to IBM's fifth annual Cyber Resilient Organisation Report, enterprises deploy approximately 45 cybersecurity-related tools on their networks. That's far too many separate apps to manage – more windows than most multitasking computers can display at once. Amalgamating and interpreting data from different sources within a single solution is important to increase the security of today's complex organisations. By aggregating security and configuration data on an ongoing basis, potential entry points and attack routes can be addressed before they're overwhelmed.

As the threat landscape continues to grow, effective vulnerability management will be essential to protecting businesses. Instead of prioritising "big threats" with the top CVSS scores, security teams need to detect and address exploitable vulnerabilities with insufficient security controls efficiently. Security teams that proactively identify and remediate exposures will ultimately make MaaS less effective and lucrative for both novice and experienced cybercriminals, reducing the pool of threat actors by raising the skill levels, efforts, and resources necessary to succeed. ■

## Network defence is easier when attackers don't see a target.

Zero Trust Network Access for servers, serverless and service mesh.

<https://enclave.io>



ENCLAVE

# DATA centres Ireland

**16-17 Nov 2021.**  
**RDS, Dublin**

**Infrastructure. Services. Solutions.**

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

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

### EVENT HIGHLIGHTS INCLUDE:

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

Entry to ALL aspects of DataCentres Ireland is FREE

**Meet your market**

For the latest information & to register online visit  
**[www.datacentres-ireland.com](http://www.datacentres-ireland.com)**



# Public v private blockchains

Jonas Lundqvist, CEO, Haidrun

A blockchain is a special type of distributed database or ledger technology, differentiated by the way it stores and manages files of information into groups of data. These so-called blocks are cryptographically signed and linked to form a chain. Each block contains a record of when it was created, producing a complete timeline history rather than the snapshot offered by traditional databases. This detailed system of record cannot be corrupted, lost or changed.

The blockchain is duplicated across all computers running a blockchain node that make up a Peer-to-Peer (P2P) network and any one of them can view the entire blockchain. Transactions or records are processed by the nodes, which verify the data and achieve a consensus on their validity. This is where the different types of blockchain start to diverge – private, public and hybrid.

A private blockchain has a single authority or organisation that ultimately retains control and no one can enter the network without proper authentication. Private blockchains are, by definition, 'permissioned' and are more suited to enterprises for reasons of performance, accountability and cost. The private blockchain platform can be run and operated by the enterprise itself or as a Blockchain as a Service (BaaS). They are usually set up where it does not suit an enterprise to allow every participant full access to the entire contents of the database. Private blockchain platforms focus on companies and institutions where the blockchain empowers and supports the business rather than individual users.

Public blockchains are fully decentralised where there is also no single entity in overall control. They typically involve their own cryptocurrency and anyone can download the software, view the ledger and interact with the blockchain. Public blockchains try to preserve an individual user's anonymity and treat users equally.

Hybrid blockchains have one foot in each of the public and private camps. They can be effective for consortiums where the members or a designated authority can determine which transactions and data remain public and which are confined to a closed group.

Blockchain technology delivers a distributed database that provides a single time-stamped version of the truth. It then uses mathematics and cryptography to provide trust and security – rather than through third parties – and relies on an accessible and open user structure to confirm all is well.

So, private blockchains adhere to the original principles but some use cases can look more like centralised, controlled networks. They offer all the distributed benefits, whilst retaining control to improve privacy and eliminate many of the illicit activities often associated with public blockchains and cryptocurrencies. Enterprises also must demonstrate full accountability, often via external audits, on the running and operation of their systems. Private blockchains can provide a much higher degree of regulation, determined and set by the administrators in line with their industry's regulatory codes.

The latest generation of blockchains use more efficient consensus algorithms and protocols; but public blockchain platforms still need many participants to provide the computing power and resources for transactions to be validated. This imposes performance limitations and comes at a variable cost, which is not – ideal when you need stable and predictable business parameters. But private blockchains solve this by defining the number of nodes to participate, making overall performance faster. In this way, private platforms are also more scalable, where nodes and services can be added on demand.

Importantly, private blockchains do not need

to use cryptocurrencies or native tokens and any association with cryptocurrencies, good or bad, is not part of the private solution. So, less energy, fewer resources and fewer participants are required to run one.

Arguably, a private blockchain with a centralised authority could be more prone to data breaches. However, identity management and pre-determined access to the data and transactions, enable private blockchain administrators to control who sees what and under what circumstances. Adding blockchain technology provides robust security, making it ideal for many enterprise operations such as supply chain management.

Interoperability has always been the

missing link in distributed ledger technology. Overcoming this hurdle to seamlessly interact and exchange information between data siloes is the key to mass adoption for blockchains.

For now, public platforms drive most of the news headlines. However, private blockchains look set to become the main contributor to blockchain market growth and will no doubt retain the largest market size in 2021, according to Gartner. They provide more opportunities to utilise the technology for B2B use cases and they deliver higher efficiency, privacy, reliability, and transparency. Security is enhanced through Public Key Infrastructure (PKI) encryption and Key Management solutions, allowing the private keys only to be

accessed by their owners in the organisation. Large enterprise blockchain solutions will be custom developed according to their specific business needs and SMEs will take advantage of cost-effective pre-packaged solutions.

Blockchain is rapidly moving mainstream across sectors from financial services, supply chain and telecoms to health and insurance. Gartner forecasts that the business value generated by blockchain will grow rapidly, reaching US\$176BN by 2025 and US\$3.1tn by 2030.

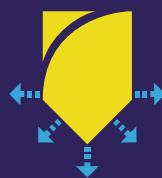
The question is whether enterprises will be happy to adopt the traditional public model or chose to embrace the private or hybrid approach. ■

## arcserve®

### Strengthen your data resilience with Immutable Backup from Arcserve

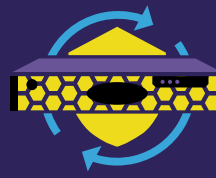
Buy an Arcserve Appliance secured by Sophos,  
and get **OneXafe immutable storage!**

Arm your business with a multi-layer protection approach to strengthen your overall data resilience. Arcserve brings you data backup, recovery, and immutable storage solutions with integrated cybersecurity to defeat ransomware and provide the best-in-class data management and data protection solution in the market.



#### Arcserve UDP Data Protection Software

Unified data and ransomware protection to neutralize ransomware attacks, restore data, and perform orchestrated recovery.



#### Arcserve Appliances

All-in-one enterprise backup, cybersecurity, and disaster recovery, with multi-petabyte scalability.



#### StorageCraft OneXafe Immutable Storage

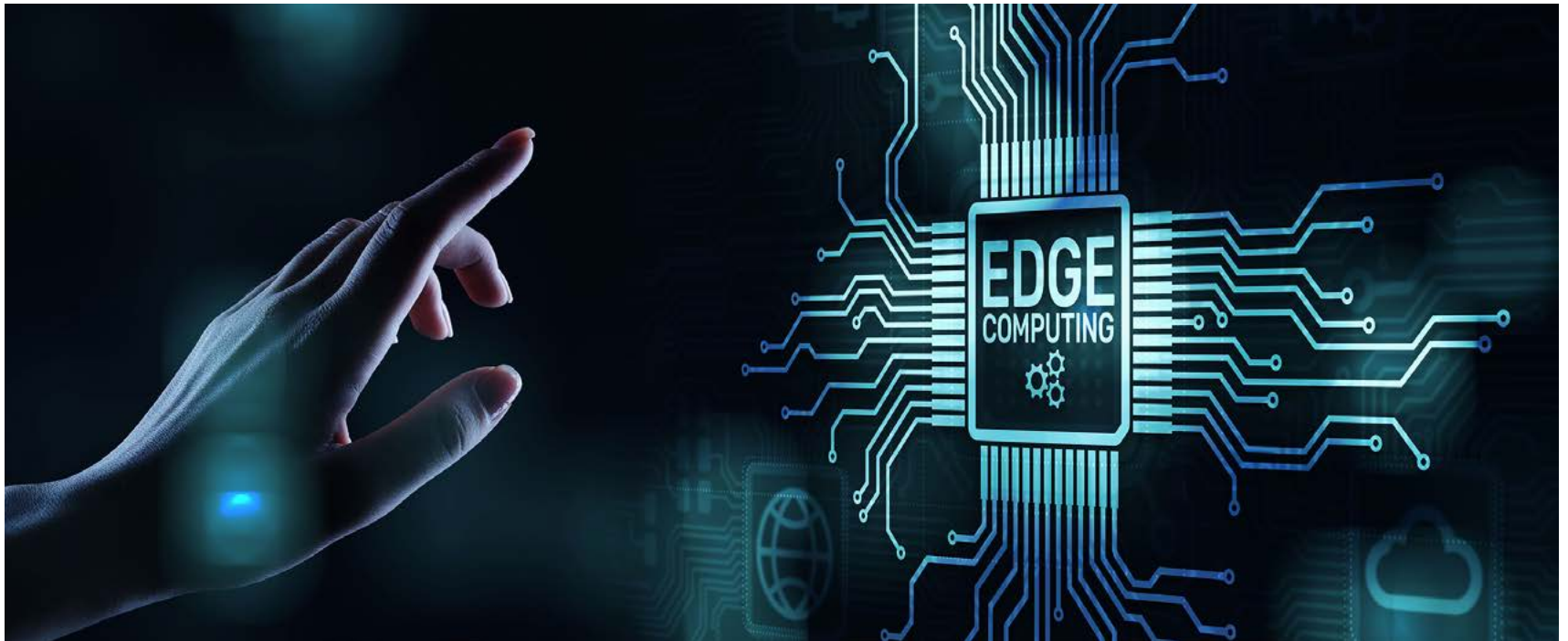
Scale-out object-based NAS storage with immutable snapshots to safeguard data.

**Get multi-layer protection!**

SCAN HERE →







# The tale of the cloud and the edge

What's the difference? Will one replace the other? Can they co-exist? We ask the experts

**Is edge computing just a fancy new name for a type of cloud computing, or is it totally different?**



**Peter Ruffley, CEO, Zizo:** The fundamental difference between edge and cloud computing is that edge computing means dealing with the data where it is produced or collected, whereas cloud computing means moving all of the data onto the cloud before you do anything with it. There are many different types of computing devices that can be utilised in a variety of scenarios in a highly

cost-effective way. This means that the collection and processing of data can take place in many circumstances which previously would have been considered unfeasible. For example, small devices which use less than 40 W of power can be deployed in remote environments, powered by wind or solar power. They have sufficient capability to store and process huge amounts of data on their own.



**Mark Richman, principal product manager, iManage:** Rather than thinking of edge computing as something "totally different", it's more useful to view edge computing as part of the push-and-pull that has shifted computing power from the client to the server and back again over the course of the modern computing era. First, computing power moved from the mainframe to the PC, the second shift was to client-

server computing, then it moved from the PC to the cloud. Now the pendulum is starting to swing back in the other

direction, towards the edge. It's important to keep in mind, however, that most edge devices can't accomplish much on their own unless they have access to the cloud, so in some ways, edge computing is just a fancy new name for a type of cloud computing. Bottom line: this is just a different version of the same computing power story that's been playing out for the past 70 or so years.



**Iain Davidson, senior product manager, Arkessa:** Edge computing is different. It reflects where processing is done in a network or system context. For example, with edge computing data is captured, processed and actioned on the sensor device, or perhaps in a gateway device or server which is located on-site. In contrast, cloud computing involves moving data

over internet links to data centres for processing. Edge Computing is capable of more real-time decision-making but requires more compute capacity and power in the sensor. Whether Edge or Cloud is best, as well as the relationship between Edge and Cloud, will depend on the application requirements. Distributed Multi-access Edge Compute (Distributed MEC or DMEC) is a hybrid approach which we will touch on later. Wireless Logic partners with Vodafone and AWS to bring DMEC capabilities to market.



**Russ Kennedy, chief product officer, Nasuni:** Edge computing is totally different. Cloud computing is more of a centralisation of computing tasks, whereas edge computing is purely distributed and designed to capture the massive amounts of data being generated at the edge in real time. We're going through a period of massive technological change. Think about the volume of data being generated by autonomous vehicles. The sensors are

capturing data in real time, and the vehicle needs to make decisions in real time, right there at the edge. Edge computing is highly transactional. You have huge volumes of data coming in at highly accelerated rates, and you need to be able to capture, analyse, and make decisions right there on the spot. We see something similar with enterprise file storage, as large global organizations need storage resources to be accessible in geographically distributed locations. An office in London shouldn't have to reach over to Los Angeles to access data – these files should be available at the edge, in London. At Nasuni we embrace that edge architecture, and the needs of the edge, while also recognising that there is a need to centralize this data for protection, security, collaboration, and analytics. The idea is to make data available at the edge for people working in distributed locations but also be able to centralize this data back to the cloud.



**Tim Mercer, CEO, Vapour:** While edge computing complements the cloud and can form a key part of an organisation's tech infrastructure, it is totally different. As the name would suggest, it sits on the edge, as opposed to in the private, public or even hybrid cloud domain. Typically used to run applications with real-time, sensitive data, it provides access to that data, locally, so that you

can do what you need to with it, and when you're finished, it is sent to the cloud to be managed and supported. It is (or should be) used in instances when sending that real-time data to the cloud would be too slow, too expensive, or cause latency issues.

**Do edge and cloud computing suit certain industries better than others?**

**Peter Ruffley, CEO, Zizo:** The applicability of the two solutions isn't decided by industry or sector. Instead,



it's to do with the amount and value of the data being processed, as well as the availability of connectivity. In circumstances where there is good connectivity and the data has a known value, such as the financial sector, then cloud-based solutions will be very effective. Some industrial scenarios may prevent the implementation of Wi-Fi for security reasons, so an edge solution would be the only possible solution. Other industrial sectors, for example, the maritime industry, would deploy an edge solution because there is no consistent connectivity on the majority of merchant shipping.

**Mark Richman, principal product manager, iManage:**

There are certain industries and applications that initially jump to mind when thinking about edge computing, IoT being a prime example. There's a lot of innovative work in particular being done on the "industrial IoT" side of things, with small computing devices that can be placed on trains, tractors, earthmoving equipment, and other heavy machinery. These devices can gather real-time metrics on location, performance, and environmental conditions, and then send that data en masse to the cloud where it can be further processed. This is far from the only setting taking advantage of cloud and edge, however. There's plenty of edge and cloud computing taking place in knowledge work industries, where there are a combination of applications that professionals use every day that either run on a user's device (edge) or run in a purely web version (cloud). Again, it's really the combination of edge computing and cloud computing that's key, and there can be different kinds of expressions of that combination across different industries.

**Iain Davidson, senior product marketing manager, Arkessa:**

Yes, although it is perhaps less about industries and more about application requirements. Applications that require highly responsive, real-time control such as manufacturing, robots, AV, next-gen micro-mobility, remote crane operation, or even remote surgery all have a fundamental safety-critical dimension that translates into real-time processing, ultra-low latency, and ultra-reliable communications. In these circumstances, edge computing combined perhaps with private LTE or 5G networks is the best fit. In contrast, large enterprises managing campuses, energy networks, road networks, or cities using large fleets of devices will almost certainly adopt a cloud-based approach. The common theme in these cases is capturing, merging, and processing sensor inputs from a wide array of sources to determine near-term actions, to build a predictive maintenance model (machine learning), or to investigate any failures. Having data in a cloud environment for both near real-time aggregation, processing, and offline processing makes sense. For example, consider a town with air quality, noise, traffic, weather, lighting, parking, EV charge points, micro-mobility fleets, and security monitoring systems. CCTV aside, these sensors will typically produce small amounts of regular data. The economics of large fleets dictate that managing the cost and maintenance of remote devices will be important. As such they will be connected and managed via 4G or 5G technology, likely a mix of lower power technologies (like LTE-M or NB-IoT), or higher performance 4G/5G in some cases like law enforcement (body cameras) or HD CCTV (e.g. image recognition, detection of littering and so on). In reality, a hybrid approach (edge and cloud) is most likely required depending on the application requirements.

**Russ Kennedy, chief product officer, Nasuni:** Any industry in which data is being generated from sensors and machines at the edge is suited for this type of architecture. I mentioned autonomous vehicles, but Healthcare is another key example, as you have medical equipment, sensors, and various other devices providing information that needs to be processed quickly to inform decision making. We see the need for edge computing with some of our large manufacturing clients, too. If they want to optimize processes, they need to be able to analyse data in real time.

**Tim Mercer, CEO, Vapour:** Edge computing is particularly relevant in scenarios that require rapid access to real-time data. IoT strategies, driverless cars and health wearables are all great examples where the data better resides on a device on the edge. Many people wouldn't consider their mobile phone as an edge device, for example. But my phone gives me real-time local access to the data produced by my Garmin watch (a wearable), and that data is then stored in Garmin, when I no longer need it. The new BMW iX comes with a 5G SIM which enables the sharing of live traffic information with other 5G cars nearby, to inform drivers' chosen routes. In fact, 5G has been a major driver



in edge computing advancements, as it presents a speed of connectivity that just wasn't possible before.

## Why is the edge often touted as the cloud's successor?

**Peter Ruffley, CEO, Zizo:** I don't think it's right to say that edge is a successor to the cloud – instead, it's more of a realisation that cloud solutions aren't always able to be provided in every scenario. We talk constantly about the connected society, but in many places and situations, there may not be a cost-effective and reliable connectivity solution in place. That is a prerequisite of any potential cloud-based solution being implemented. Alternatively, edge-based solutions offer a way forward when no cloud-based solution can be provided. In the days of big data and then IoT, there was a rush to collect all data, without much thought about the cost of doing that, storing it and what its potential value might be. This resulted in the creation of huge amounts of data, stored in such a way that made it difficult to extract anything from it, least of all business value. Edge computing is developing as a more thoughtful, structured and potentially lower-risk approach to those data-rich projects.

**Mark Richman, principal product manager, iManage:** I don't think edge is the cloud's successor, because there's always going to be massively more computing power available in the cloud than is ever going to be available on any single edge device. Even though computing power has increased exponentially, the massive parallel processing power of a cloud is always better. To me, the edge being touted as the cloud's successor is highly reminiscent of the idea that PCs were going to kill the mainframe back in the 80s. PCs didn't kill the mainframe; the mainframe just evolved and became the cloud. So, edge computing is not going to be the cloud successor: the two are going to continue to work together, just in new and different ways.

**Iain Davidson, senior product marketing manager, Arkessa:** With advances in cellular networks and microprocessor technology, Edge computing is now more economically and technically viable so it is undeniably on the rise, but it won't replace cloud computing, it will complement it.

Cellular networks now provide options for low power, high-density sensor deployments as well as low-latency, high-speed connectivity. The computing density of microprocessors continues to increase and combines general CPU performance with image processing and AI engines. Edge is on the rise.

**Russ Kennedy, chief product officer, Nasuni:** I'm not sure it should be touted as the cloud's successor. Both will continue to exist because they satisfy distinct needs. Edge computing is all about rapid capture and processing of information where it's generated. Cloud is more about the centralization of resources and, in the case of cloud file storage, all the amazing things you can do once your data is centralised in a single, globally accessible namespace.

**Tim Mercer, CEO, Vapour:** I've read stat after stat about edge computing, with one claiming that almost 80% of decision makers will use it over the next 12 months. These figures aren't surprising, because, in all honesty, I think edge computing has been around for some time – it's just got a shiny new name badge. And I don't think the debate is as simple as one or the other, as the technologies are complementary. It doesn't matter if a customer is running 30 applications – if there's even one that they're heavily reliant on, is particularly complex or they require data from in real-time, we will talk to them about the ability to manage it locally, before sending the data to the cloud for storage. We've done this for some time. As should always be the case in the tech space, decisions should be made on a case-by-case basis.

## Can the two co-exist peacefully?

**Peter Ruffley, CEO, Zizo:** Absolutely, the two complement each other very well. Businesses can benefit from having a collaborative situation where, for example, low value data was collated and analysed at the edge and then the results are sent up to the cloud-based solution for aggregation and overall analysis. This can provide cost-effective and robust computing solutions. It seems to me that there is a role for both of the solutions going forward. There is no doubt that having high-value complex AI and ML solutions available on the cloud is going to be very



important in the future, but the reality is that to get the most from them, you only want to use them on data that has known value.

**Mark Richman, principal product manager, iManage:** Absolutely. Edge and cloud are two computing approaches that work together – they’re complementary. You might have one application that has a greater reliance on the edge and one that has a greater reliance on the cloud, but these two approaches will continue to work together, co-existing peacefully.

**Iain Davidson, senior product marketing manager, Arkessa:** Yes. They have to – and in fact, there are hybrid solutions available today which combine the two in a complementary fashion. Take DMEC for example; Wireless Logic partners with Vodafone and AWS to bring Distributed Multi-access Edge Compute (Distributed MEC or DMEC) capabilities to market. DMEC enables the cloud processing to be performed at the edge of the mobile core network which helps significantly reduce latencies associated with moving data between device and cloud.

**Russ Kennedy, chief product officer, Nasuni:** There is absolutely a place for both of them to exist and evolve. I see them as complementary not competitive solutions. From the cloud perspective, some or all of that data being generated and processed at the edge might need to be captured preserved for post-process analysis, legal analysis, compliance, or general data protection. Nasuni has embraced the idea that edge and cloud are complementary, and a result we’re able to provide our customers with the performance they need at the edge while simultaneously preserving, protecting, and securing that data in the cloud – and as a result making it available for analysis in a post-processing environment. The data might not exist without the edge resources, but none of these additional benefits would be available without the cloud.

**Tim Mercer, CEO, Vapour:** Yes. Linked to what I’ve already said, it doesn’t have to be ‘one or the other’ and decisions should be made according to factors such as cost, security, performance, scale and so on. When it comes to the public versus private cloud debate, we’d never categorically say one or the other. It’s much the same in terms of edge versus cloud computing, but it

needs a confident, customer-focused, technology agnostic specialist to truly advise on what’s right for the business, and not just push the solution that’s most familiar to them.

## Does cloud or the edge have an advantage in 2021?

**Peter Ruffley, CEO, Zizo:** Right now, you could always design and deploy an edge-based solution, but you simply can’t say that about the cloud. There are also question marks over the costs of cloud and understanding what they may be as solutions scale up. There has been a tacit understanding because cloud solutions are now very widespread that somehow they have been commoditised, and therefore, the costs have come down. This may not be the case as solutions grow larger and more complex, as, in turn, the incremental costs of cloud storage can start to rise steeply. This can be a problem if you are holding large amounts of low-value data.

**Mark Richman, principal product manager, iManage:** I think I reject the premise of the question: to my mind, it’s not a matter of one having the advantage over the other. Ultimately, these two things work together, and you can lean more towards “edge” or more towards “cloud” depending on your application and what you’re trying to achieve. Most applications these days would really struggle to deliver a robust solution relying strictly on edge computing, because they fundamentally rely on the power of the cloud to aggregate all of the information that is generated at the edge. There certainly could be applications where you could have edge devices that potentially communicate entirely in a peer-to-peer fashion with no centralised cloud, but the applications for that are going to be very specific and somewhat limited. At the end of the day, the choice of cloud or edge really depends on the application. There’s value for each, and there’s value in combining them in different proportions, based on what you’re actually trying to achieve.

**Iain Davidson, senior product marketing manager, Arkessa:** Edge computing will have some advantage in the sense that it enables genuine transformation in IoT. That said, it will also drive new distributed edge (DMEC) and traditional cloud-based workloads. Edge compute devices

will still share data with cloud-based systems after all and in many scenarios, a hybrid approach will be adopted.

**Russ Kennedy, chief product officer, Nasuni:** There is absolutely a place for both of them to exist and evolve. I see them as complementary not competitive solutions. From the cloud perspective, some or all of that data being generated and processed at the edge might need to be captured preserved for post-process analysis, legal analysis, compliance, or general data protection. Nasuni has embraced the idea that edge and cloud are complementary, and a result we’re able to provide our customers with the performance they need at the edge while simultaneously preserving, protecting, and securing that data in the cloud – and as a result making it available for analysis in a post-processing environment. The data might not exist without the edge resources, but none of these additional benefits would be available without the cloud.

**Tim Mercer, CEO, Vapour:** The application drives this, not the solution. So, it depends on the scenario. And customers – certainly those with savvy CTOs – are asking more probing questions to ensure they receive the right recommendations. They’re talking to vendors about how to better manage their applications, how these applications traverse networks, what they do inside businesses, how they can affect overall network performance, and so on. There’s also a larger appetite for making corporate networks more secure, agile and scalable, and for many businesses, cloud and edge will both have a role to play.

## What are the key things an enterprise should consider when choosing a supplier?

**Peter Ruffley, CEO, Zizo:** Before businesses think about choosing a supplier, they should have constructed a strong business case. In the case of IoT, something that both edge and cloud solutions are available for, you should have clearly identified what level of value you expect to get from the solution. As well as considering what the potential value of the data that you are collecting might be, you have to seriously consider which pieces of the solution are in place and how much it will cost to put them in place if they are not.

For example, if you are looking at implementing a cloud-based solution, but it will involve the installation of factory-wide Wi-Fi, then it may represent too much risk, such as too much money being spent before the value of any return can be assessed. Edge-based solutions can represent a lower risk in determining potential business value.

**Mark Richman, principal product manager, iManage:** Really, it depends on what the end user is trying to achieve. That being said, as with anything, security is key, especially as more and more data is gathered at the edge. That means tens or hundreds of different places to secure rather than just one central location like the cloud. How is data actually being secured at the edge? Updateability is a big part of this larger security aspect – making sure that those edge devices have ways of being patched or updated as security improvements continue to evolve. Likewise, upgradeability is something for enterprises to carefully consider: what are the implications when newer and better capabilities come along for increased processing power at the edge? How are they going to be able to upgrade these edge devices as new capabilities evolve? What happens if an edge device breaks, and you need to replace it – how are you going to do that? There are a lot of factors that need to be considered, no matter what application you’re trying to implement.

**Russ Kennedy, chief product officer, Nasuni:** Enterprises should start by asking a few fundamental questions. What is your specific need? What are you looking to do at the edge? What types of data are you going to be processing and analysing? What outcomes are you looking for once this data is processed? Once you understand your needs, you can start to look at vendors. From a storage perspective, which is where we operate, and an analytics and processing perspective, there are going to be lots of choices, so I’d start with your needs and match vendor capabilities to that list. ■



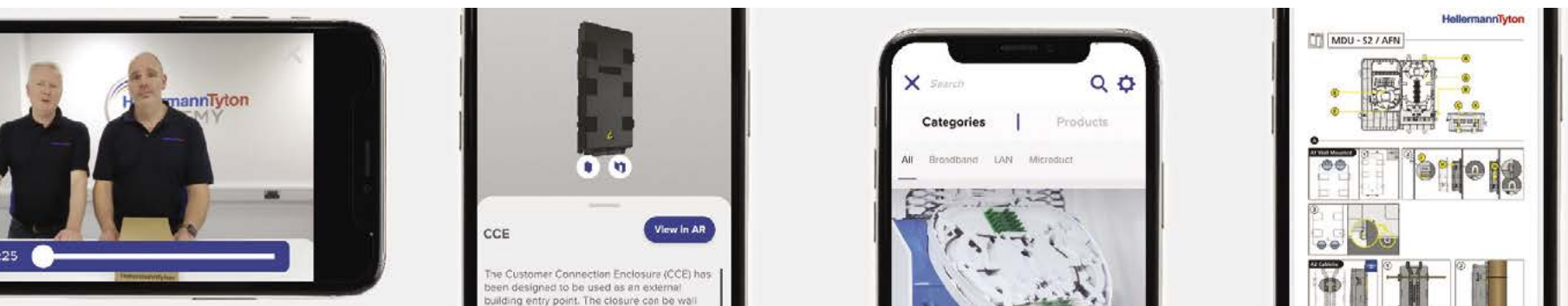


## HT CONNECT

The perfect  
product  
information tool.

**MADE TO CONNECT**

**NEW  
APP!**



## Download our NEW Mobile App

The HT Connect App from HellermannTyton is the perfect product information tool.

Using Augmented Reality (AR) technology through your mobile phone or tablet, you can see a number of selected products from the HellermannTyton product range in a live environment.

The app is designed to give you a closer look at our products as well as giving you additional information including datasheets, installation guides, installation videos and links to website.







# What role will 5G play in delivering critical communications?

Jason Johur, TCCA board member and chair, TCCA's Broadband Industry Group

**5**G networks promise greater capabilities to critical users but further specification work is needed to ensure their unique requirements are met. A new white paper from TCCA, the global organisation for the advancement of standardised critical communications technologies, says that ultimately, 5G will enable cooperation between critical users to become more efficient and effective. As a result, the safety of first responders and the communities they protect will be enhanced.

The white paper addresses a number of key questions raised by the critical communications community on the role of 5G, including how it compares to 4G LTE, the initial use cases, the expected impacts on user operations and the likely market availability of such solutions.

5G opens up the potential for a range of new services, most notably driven by 5G's ultra-reliable low latency communications and support for massive machine-type device deployments. Use cases that will benefit users include enhanced situational awareness through the use of advanced video recognition capability and artificial intelligence-powered analysis of data. For first responders, this means control rooms will have a far more accurate view of a situation and can better allocate people and resources. Information can be shared between agencies seamlessly, via cloud-based application platforms.

In terms of standardisation, several of the 5G network enablers have been specified in 3GPP Releases 15 and 16. However, some enablers critical for use cases such as broadcast and device-to-device communications are still in development and not expected before 2023. The white paper outlines the expected timescales for this work and warns that although there are some early 5G devices available now, those suitable for critical communications will not be available for at least another year. Similarly, while applications that could benefit critical communications users have been designed for 5G networks, these are not yet mature or proven enough for mission-critical operational use.


While 4G LTE delivered a paradigm shift in critical communications versus previous technology generations, 5G brings evolutionary change in terms of speed, latency, security, breadth of use cases and quality of service. There is a growing global ecosystem committed to driving further standardisation and development of 5G features and services to ensure the networks, applications and devices will fully support the crucial work of critical communications operators and users.

"There is no doubt that 5G has earned the attention of mission critical communications customers with its promises to address their demands for flexibility and higher speeds to help the evolution of their traditional voice-



centric communications and adopt disruptive multimedia features like prioritised video sharing, real-time data analysis and location-based services - all under an augmented focus on reliability, capacity, security, and cost efficiency," says Ildefonso de la Cruz, principal analyst - industrial and government critical communications at Omdia. "We have started to see examples of 5G deployments taking business automation

to the next level in other industries. However, the ongoing 3GPP standardisation efforts are necessary to overcome gaps such as direct-mode communication and support for MCX services to enable 5G to make significant inroads into the critical communications market. Read the white paper here."

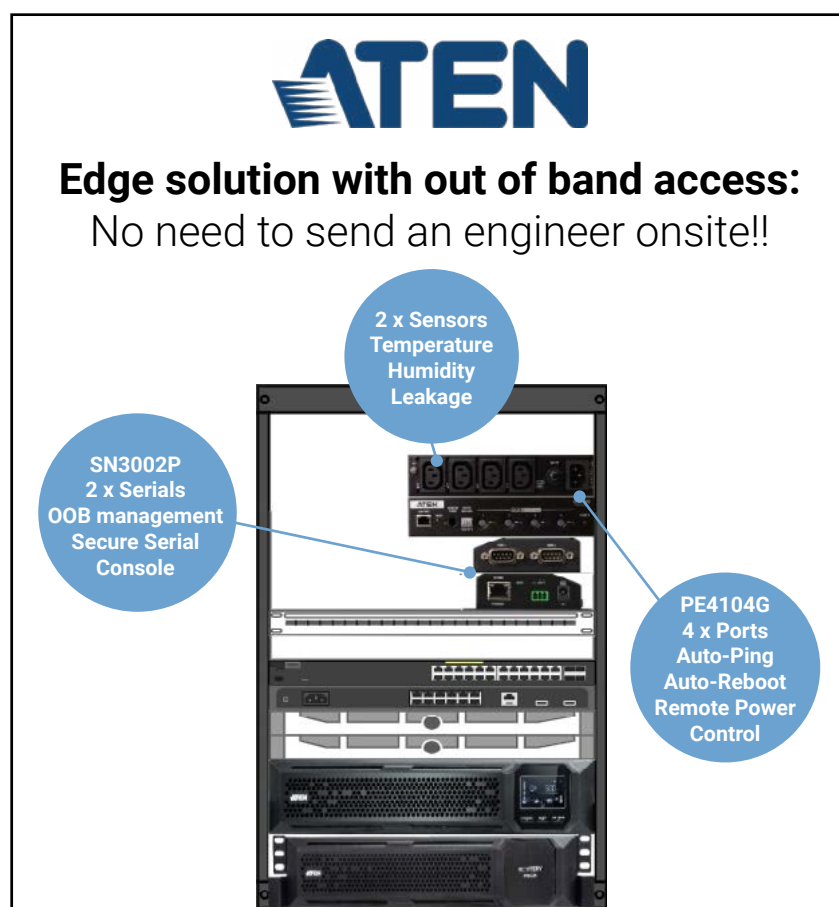
Jason Johur is head of strategy and market development for Ericsson's mission critical networks business. 



**RM**™

"Whilst they may be in the background, RM are still there for me. The people I speak to know me, I know them, and they know our network. It works really well."

**Don't take our word for it.**



**ATEN**

**Edge solution with out of band access:**  
No need to send an engineer onsite!!

- 2 x Sensors  
Temperature  
Humidity  
Leakage
- SN3002P  
2 x Serials  
OOB management  
Secure Serial  
Console
- PE4104G  
4 x Ports  
Auto-Ping  
Auto-Reboot  
Remote Power  
Control

UPS - OL3000HV

- Revolutionary PDU: Exclusive Auto Ping and Auto Reboot to remotely power cycle.
- Remote access to 2 port Serial Console Servers with POE and Power Redundancy.
- Perfect for Small Corporate Rack or 5G installation

Phone: 01753 539121 | Email: sales@aten.co.uk





## Cloud native storage: lifting the burden off I/O managers in the hybrid world?

*Russ Kennedy chief product officer, Nasuni*

**W**eb outages and ransomware attacks on health services and charities grab the headlines for their cynicism. But in a world of rejigged IT and hybrid working, I/O teams need to focus on longstanding challenges, such as 'under the radar' data loss, file storage upkeep, and storage capacity planning, to safeguard their critical information and chart a path to recovery.

Managing hybrid working and infrastructures that were quickly reworked in 2020 continues to pose risks for networks and data. Whether outages from Content Delivery Networks, disruption to high-profile apps, or loss of entire data centres, these incidents show the dangers that organisations with multiple cloud applications and hybrid working models are facing.

Companies may lose and misuse data through manual processes and human error. The Information Commissioner's Office data security trends report for Q4 2020-21 shows that instances of information being compromised by being sent to the wrong person outnumbered ransomware attacks by almost 300%. With Government data showing 85% of employees want to retain some form of hybrid or remote working, such challenges aren't going away.

As economies take their bumpy path out of restrictions, businesses need fresh thinking on sharing, storing and recovering critical data. They could also benefit from simpler business continuity planning and recovery processes for information assets to become more responsive in general. The answers to these questions lie within the new generation of cloud storage platforms.

Until recently, maintaining data in the cloud wasn't a credible strategy for many I/O professionals. Firms cited performance issues like questionable redundancy and data fragmentation. However, the latest cloud native platforms have overcome these issues and their ability to be deployed in hybrid, multi-cloud and multi-region environments, helps create a consistent storage experience across different infrastructures.

Organisations with on-premise file sharing are tied to duplicate locations and co-located DR sites which remain complex to manage. Data has to be regularly replicated to support sharing across locations and restoring data after outages can take days. With cloud storage platforms, enterprises can consolidate file servers, move unstructured data to the cloud, and manage multiple file servers from a single console.

This type of product delivers edge caching combined with SMB and NFS file access, built-in backup, disaster recovery, and multi-site file synchronisation, that eliminate the headaches associated with managing installations such as on-premise Windows File Servers. Cloud native strategies also simplify digital transformation programmes, especially where users' service expectations of core applications are still high but IT budgets have often been cut.

Cloud storage is also changing storage's image from business cost to business enabler; where a company has been running on-premise file storage architectures, a server outage at a remote location might mean that everyone there, and any connected sites, can't access their files and lose vital productive time.

The latest cloud-based file storage platforms avert such downtime for three main reasons.

First, they keep immutable copies of every file and provide a local access point, with caching of active files for fast access. Secondly, these systems take granular

snapshots of local data every few minutes and send them to the cloud to be stored in an unalterable format — a more efficient approach than daily backups that are common with on-premise systems.

Thirdly, such platforms continually track file usage by individual location or edge appliance; if a server fails, the IT team can set up a new edge appliance connected to a working server, along with access to the relevant files. File systems can be reconstituted with uncorrupted data for virtual appliances locally after any incident with users regaining file access in less than 30 minutes. This in-built disaster recovery ensures that any location or the wider

organisation need never lose access to shared project files, and it provides welcome recovery from crippling ransomware attacks.

Cloud native storage's nature means that organisations can operate simpler business continuity plans. In addition, IT professionals will find infrastructure and storage capacity planning much simpler, because they can add storage without having to make capacity calculations, or pay additional management costs, as often happens with on-premise models.

The huge attention given to how companies manage 'collaboration by Zoom or Teams' and hybrid work fatigue has overshadowed the need in a post-pandemic economy for

companies to find smarter ways to share their knowledge assets — globally or locally. Companies that need to rapidly consolidate or expand their operations post-pandemic can now use a cloud native approach to consolidate file storage and quickly spin up capacity for new projects. Their hybrid models work better while becoming more responsive overall to customer needs.

Whether an organisation faces a malicious attack or a service outage, cloud native file storage enables it to recover data in minutes. It is also helping companies achieve the more flexible information-sharing and simpler business continuity processes needed in the new world of hybrid work. ■



**FREE Site Survey available**

## Simple cloud-managed networking for education

The fully hosted cloud-managed networking solution with a free dedicated app and a pay-as-you-grow subscription model.

Nuclias has a full range of Access Points and Switches that can provide you the wireless solution you need;

- Wi-Fi 6 – Future proof with lightning fast Wi-Fi 6 solutions, DFE connect the classroom approved
- High Density 4x4 – High density AP's for areas requiring extra bandwidth
- Outdoor/Waterproof – AP's that can be deployed to provide Wi-Fi outdoors or where waterproofing is needed



FIND OUT MORE - SCAN THE QR CODE BELOW



For a free site survey call us on  
0208 955 9081 or email [UKI-sales@dlink.com](mailto:UKI-sales@dlink.com)  
For more information visit [www.nuclias.com](http://www.nuclias.com)

**D-Link®**





# Spectrum for sale – the benefits of private wireless networks

Reliable, effective, wireless networks have become a critical component to day-to-day life in our pandemic environment. Tina Yates, EMEA business manager, Nuvias Group, discusses why strong, reliable wireless networks are not just critical to the economy, but in enabling the future of IoT



many businesses require.

## Access to a private network

Private networks require access to spectrum, a precious and finite commodity. Spectrum refers to the invisible radio frequencies that convey wireless signals. It is what enables us to make calls, message someone on our smartphones, use social media or shop online. The frequencies that we use for wireless are only a small portion of what is called the electromagnetic spectrum.

The UK and Germany have recently put some of the national spectrum up for sale. It is an opportunity for businesses and organisations to build their private networks. For many, it presents the chance to create a high-performance, efficient network in a disputed and fluid environment.

Take the following sectors as examples as to how private networks can transform their performance.

- **Airports:** We are all hoping that air travel will soon return to normal. When it does, we need to adjust to the realities of a post-pandemic world. In the new environment, airport operators need to monitor passenger flow and minimise any health risks. A robust, industrial-grade private wireless network makes effective use of Artificial Intelligence (AI) analytics. It keeps track of passenger movements, interprets temperature-sensing imagery, and monitors mask usage, all in real-time. Even in normal circumstances, efficient wireless data connectivity is vital to ensure the smooth running of an airport. IoT enabled equipment coordinates efficient bus transfers, refuelling operations, baggage handling, de-icing, and many other day-to-day issues. Real-time data can

also reduce flight delays and enhance plane turnaround times.

- **Ports:** More than 20 million containers are on the move or storing goods every day. Keeping track of their location, and the condition of their contents is critical in a global logistics chain. Many ports, however, suffer from poor or patchy wireless coverage. A private wireless network can cover all port facilities. It ensures the safe monitoring of crane mounted video cameras to check on goods, their movements, and their condition. A real-time overview of site assets, people, and vehicles is also the best way to ensure portside security and the health and safety of the operators.
- **Healthcare:** The pandemic has put a severe strain on healthcare resources. An effective wireless network can help manage and use resources more efficiently by using IoT systems to track hospital equipment, staff, and patients. It can also provide a reliable network to host automated services for the prompt delivery of medicines, for example. The healthcare sector handles a huge amount of operational complexity, and it's in such pressured circumstances that robust networks that are not subject to failure come into their own - especially when patients' lives are at risk.
- **Education:** Higher education, especially in subjects such as architecture, mathematics and other branches of science, increasingly use complex modelling applications. There is also an accelerating need for access to databases - such as those containing engineering and statistical data - as part of these courses. For students to train in a way that will prepare them to use their skills in applied environments (if they are not already doing so), they

also require access to a stable, high-performance wireless network.

- **Logistics:** As the movement of goods becomes faster, often managed to the minute or second, connecting the pieces in a supply chain is vital. This includes potentially disruptive points in the process such as customs checks. New Brexit regulations mean hauliers need customs clearance to comply with the new import-export regulations. With trucks out on the open road, good connectivity becomes vitally important when you need fast access to up-to-date electronic documentation. The connection of vehicles, goods, suppliers and customers will only increase in importance as eCommerce continues to accelerate.

## Spectrum for Sale

Nokia's Digital Automation Cloud (NDAC) creates the opportunity to take advantage of the new availability of national spectrum for private use. Its private wireless networking solution has already been successfully deployed across the world by leading airport operators, automotive, manufacturing, and energy companies.

NDAC reliably and securely connects CCTV, walkie-talkies, drones, robots, self-serving vehicles and more. Designed for industrial-grade wireless networks, it offers considerable gains in security and reliability compared with standard Wi-Fi. Beyond just peer-to-peer connectivity, it provides IoT connectivity at the highest level. It also provides a platform for the affordable deployment of 5G and related applications in the future.

If you are considering a private wireless network, now is the chance to get on board. It could be the boost and security your organisation has been looking for. ■

## INDUSTRIAL IoT

### Connected Antenna Solutions

Reliable Antenna Solutions for Data Monitoring and Remote Control.  
4G LTE & 5G-ready Cellular Solutions as well as Cellular/WiFi/GNSS  
Multiband Applications. Embedded, Fixed Site and Mobile Antennas.

Contact Us Now  
+44 1543 459555  
enquiries@MobileMarkEurope.co.uk






www.MobileMark.com





## A new era in IoT security: how organisations can combat the latest threats

**Keith Glancey, systems engineering manager, Infoblox**

The Internet of Things (IoT) is not a new concept. For years, IoT devices have been widely and deeply embedded into our homes and businesses as well as society in general. But, when the pandemic struck last year, that level of integration suddenly became a security liability for thousands of companies.

### The IoT challenge

Even before the pandemic struck, IoT security was far from easy. In fact, research discovered that one third (33%) of UK businesses believed there were around 1,000 unauthorised or non-business related IoT devices – also known as Shadow IoT devices – connected to their enterprise networks. These devices can open a business up to attack and also enable unsanctioned “lurkers” to access any given network. One of the consequences of the rise of shadow IoT was a surge of 17 million cases of distributed denial-of-service (DDoS) attacks across the globe in 2020 alone.

As remote working increased during the pandemic, so too did the use of remote and IoT devices, increasing the threat they pose to organisations. The average home

today has 11 IoT devices connected to its network—many of which have weak or non-existent security protocols. Each of these devices will be unknown to the IT team and, as such, could provide a vector through which malware can enter an employee’s home network and then move laterally to infect the corporate network as well. Given that businesses can’t easily enforce corporate security policies on devices that sit outside of their infrastructure, this is opening up the floodgates and putting businesses at increased risk from attacks such as phishing and malware.

To add to this, many employees are naturally less risk-averse in their home environments. They will willingly use their work devices to engage in behavior that they might think twice about in the office, such as browsing social media, shopping or streaming entertainment services. What they might not realise is that this use of insecure Wi-Fi connections, unsanctioned applications, and browsers with insecure plug-ins has the potential to compromise the whole business network.

While the government is no longer instructing people to work from home, it has been reported that many businesses

do not plan to rush back to the office. In fact, 84% of UK businesses plan on making a permanent change and implementing a flexible or fully remote strategy moving forward. With some form of remote working here to stay and IoT devices set to continue proliferating in the future – the latest estimates project there will be over 21.5 billion IoT devices by 2025 – failure to address these security issues now could spell disaster in the long term.

### Getting the upper hand

One of the most powerful ways that IT teams can protect their network against shadow IoT threats is by increasing visibility. This is where DNS (Domain Name System) tracking can help. As one of the first services that devices use when they connect to a network, DNS knows exactly what every IoT device is doing and provides a viewpoint of the entire organisation through a massive pool of forensic data. It doesn’t rely on a device being authorised or known to IT. Instead, DNS simply needs a device to access the internet.

In fact, by merging DNS, DHCP, and IPAM, businesses can address many of the IoT challenges that come along with

our current remote working landscape. These three technologies – also known as DDI – can pinpoint threats at the earliest stages, identifying compromised machines and correlating disparate events related to the same device. By providing an up-to-date view of all devices connected to a network, regardless of location, they help to diminish some of the strain placed on IT professionals. They can even help teams to automate the provisioning of security services on remote endpoints, which removes the need to ship devices back and forth for on-site patching and allows organizations to secure users working from home.

As businesses of all shapes and sizes become increasingly remote and borderless, the IoT threat has never been more real. Defending from the network edge should be a priority for all security teams moving forward. Using core infrastructure like DDI will give organisations the upper hand and enable them to protect their networks and their employees, no matter where they’re logging on from.

### PRODUCTS

Networked computers are constantly monitored and managed – and most are protected by a firewall – yet many IoT devices are simply added and ignored, says **Watchguard**. They may have default passwords and no regular patches which can open a backdoor to the network. WatchGuard says its new Firebox M290, M390, M590 and M690 units deliver increased security, fast performance and accommodate network changes and

additional IoT devices.

They have, it says, processing power to handle encrypted and HTTPS traffic from networks plus thousands of IoT devices. Watchguard says a Firebox makes it possible to place IoT devices on segmented networks or VLANs with policies to prevent unauthorised remote access. Only appropriate IoT applications devices can run. And, says the company, any increased traffic is spotted, indicating if



a device has been compromised and used to extract data.

Watchguard Cloud is used to create, deploy and manage IoT security policies, including a 30-day view of log data, fast log search and automated reporting. [watchguard.com](http://watchguard.com)

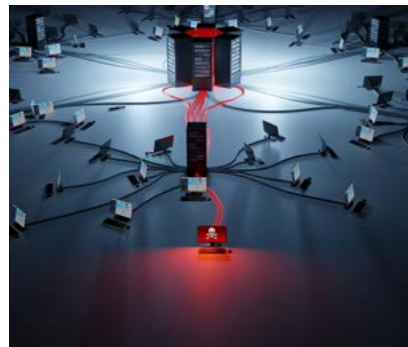
Security for IoT devices is delivered on the basis of prevention, not detection, says the maker of **Armored Client**.

**SentryBay’s** product is a single, one-time software download for customers with remote workers and allows BYoD. It is said to protect endpoints of all types including domestic and industrial IoT devices. The company says it securely wraps selected applications and data and neutralises the impact of info-stealing malware. SentryBay says it uses a secure application framework and a layered approach to protect

devices at kernel level allowing it to grab data first and transmit it to the application, irrespective of any undetected threats.

For example, to guard against keylogging – a major risk – it says Armored Client will feed false, scrambled data to the malware. To combat another attack, screen-grabbing, it will send no capture or a blank screen.

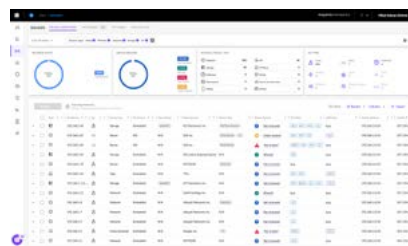
Armored Client, it says, continuously monitors for tampering and that features and configurations, centrally managed, can easily be switched on and off. [sentrybay.com](http://sentrybay.com)



Every endpoint connected to a network is found and fingerprinted by Singularity Ranger, says **Sentinel One**. Then machine learning algorithms identify the operating system, type and role of each to enable blocking of unauthorised endpoints. Cloud delivered, it is said to give up-to-date information on – and better visibility into – what is on the network, so users are fully-equipped to make better risk assessment decisions. Singularity Ranger, says the company,

passively listens for network broadcast data and correlates all learned information within the backend to fingerprint known and unknown endpoints, revealing vital information about IP-enabled endpoints and producing inventories in seconds across a region or the globe. Suspicious endpoints, including IoT, can be isolated with a single click.

It is said to be easily implemented and administrators can specify a different policy for each network and subnet



if needed and choose between auto-enabled scanning and requiring explicit permission. [sentinelone.com](http://sentinelone.com)

IoT devices often remain invisible on enterprise networks because, unlike traditional systems, they can’t be easily tracked and rarely support software agents, says **Forescout**.

Its products comprise eyeSight, eyeInspect, eyeSegment, eyeControl and eyeExtend. After deployment, it says, many customers discover 30-50 per cent more devices than they anticipated. It means that they can then manage their attack surface, mitigate cybersecurity risk, achieve compliance

and manage asset inventory.

Forescout says its platform – one of the most widely deployed – arms customers with extensive device intelligence, insights, and actionable visibility. Then it helps to create policies to allow clients to accurately classify risk, detect anomalies and quickly put in place measures to foil cyber threats without disrupting critical business assets.

Its platform, says Forescout, is based on a Zero Trust (NIST 800-207) framework



that combines complete device visibility, proactive network segmentation and least-privilege access control of all digital assets. [forescout.com](http://forescout.com)

Shadow IoT devices and their corresponding risks can be uncovered with a product that takes minutes to set up, says **Ordr**.

The company says its IoT Discovery Program is a complete kit – cloud-managed IoT sensor and Ordr Core software – to get users up and running in minutes.

Following zero touch provisioning and installation of the IoT sensor, device data is sent to the Ordr Cloud dashboard, making it easy for enterprises to analyse and act upon the granular, connected device insights to drive security decisions and improve operational performance.

Ordr says there is a free 30-day trial, which can then be upgraded to a paid deployment.

It says that Ordr Core enables users to immediately reveal everything connected to the network plus the security and management risks associated with them. Based on an understanding of device behaviours and risks, customers can then enable automated actions and advanced integrations with the Ordr Premium software subscription to proactively address these risks. [ordr.net](http://ordr.net)

Nine in 10 respondents in a **Check Point** survey said their networks had shadow IoT devices – and 44% said half were connected without their knowledge. As a result, seven out of 10 reported IoT-related incidents.

The company says IoT Protect, part of its Infinity security architecture, features zero-trust policies that use device-specific attributes and risk profiles to shield networks from known vulnerabilities with virtual patching before they can be exploited. Check Point says its Infinity architecture uses continuously updated threat intelligence from the company’s ThreatCloud, which aggregates threat intelligence from hundreds of millions of sensors worldwide.

The company says IoT Protect automatically identifies and classifies every IoT device and its risk profile using discovery engines and creates perfectly suited policies with the industry’s broadest application control.

And it says IoT devices can be “virtually patched” to fix security flaws, even those with unpatchable firmware or legacy operating systems. IoT Defense Nano-Agent can also be embedded on devices. [checkpoint.com](http://checkpoint.com)



# “ Please meet...



**Corey Nachreiner, CSO at WatchGuard Technologies**

## What was your big career break?

My official cybersecurity career started when I was working in a product support role at WatchGuard. A co-worker and the manager of a threat research team spotted that I had some security expertise and a passion for it, which I shared with customers as security advice beyond their core problem. He invited me to be one of the security and technical experts on our booth at the RSA Conference. Little did I know, this was a test to see if I could become a network security analyst and join his team. I passed and set out on the path to my career in cybersecurity and current role as CSO for WatchGuard.

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

Bill Gates. I grew up when personal computers were very new and rather than saving to buy a car, like most teens, I got a job at 14 to buy my first personal 8086 machine. Gates seemed like a young upstart geek just like me, who loved computing and dropped out of college to pursue his passion and build a computer and software business.

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

Listen more than you speak. I still struggle to heed this advice, as I'm a 'talker' but there is so much value to listening. You learn more and it allows you to act on realities and not assumptions. As someone who strives to help develop the next generation of security pros, listening helps inspire trust, belonging and respect. Finally, I crave diversity of thought to make good decisions, which means you have to do a lot of listening.

## What's the strangest question you've been asked?

"Come on, tell me the truth. Are security companies making the malware to improve business?" While most people who ask this are just kidding, I've had a few who take it seriously. It's an absurd conspiracy concept of course. Few things make me as upset as criminals who use technology to steal or harm. Like most security professionals, I am obsessed with protecting tech.

## What would you do with £1m?

I'm pretty boring, so I would invest a large portion. I like the idea of getting your money to work for you. That said, I might use some of it to start a 'side-hustle' business. While I'm passionate about InfoSec, I'm also really into virtual reality (VR) and first-person drone piloting, both racing and freestyle acrobatic. I would love to start a business around these technologies as they have great growth potential.

## If you could live anywhere, where would you choose?

I'm a traveller and love to visit other countries, which makes it hard to pick one place to live. That said, I love beaches and sun, but don't like it too hot or humid. So, a place like Alicante, Spain seems ideal. I love Spain and Europe in general. That said, I truly love where I am right now. If only I could double the number of annual sunny days here in Seattle.

## The Beatles or the Rolling Stones?

What a hard question! Thank goodness we live in a world where we can enjoy and love both bands. My soul leans towards rock, but in this case, I must choose The Beatles. The Beatles had more albums that just hit the mark and Lennon and McCartney wrote music that had

a positive impact on society and spoke to me.

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

Virtual Reality (VR) Gaming. I've always wanted to work in some medium that can stir emotion and reflection in people. Good storytelling is a very important part of our society, to learn and grow, and goes well beyond mere entertainment. It helps us to grapple with philosophy, society and life. I love books and films, but many don't realise the huge storytelling power of gaming,

where interaction makes it even more impactful. When you add VR, storytelling becomes even more immersive and offers you the opportunity to stand physically in someone else's shoes, greatly increasing its ability to move humans and help us empathise. VR or AR entertainment seems like a very satisfying area to work, as I'd enjoy dealing with breaking new technology while also leading a new storytelling medium.

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

I'd like to make a positive difference in more

peoples' lives. There's lots of things I selfishly want to accomplish and do. Getting a pilot's license and flying solo is one of them. That said, when I think of the things that have really made me feel satisfied, it's when I have had a positive impact on someone else; whether it's my family, friends, colleagues or strangers. Those are the things that make a bigger impact than sky diving solo or climbing Machu Picchu. That said, flying my wife to some fancy lunch in the state next door and returning home the same day would be pretty cool.

# BIG ON SECURITY

Security matters, that's why we offer unrivalled locking solutions. With strong, integral - multipoint - locking mechanisms as standard and upgrade options which include digital key codes, proximity cards or biometric as part of a network or a standalone solution, you can be sure your equipment and data is secure when it is housed in an Environ rack from Excel.

Visit Environ:  
[excel-networking.com/environ-racks](http://excel-networking.com/environ-racks)

**excel**  
without compromise.