NOVEMBER 2022
networkingplus.co.uk

NETWORK+

Zero trust for IoT

Essential or overkill?

Mark Oakton, Infosec Partners, p6

The challenges to IoT & OT security

The IoT threat landscape is increasingly dire

Paul Keely, Open Systems, p14

Questions & answers

Don't ever take anything for granted

Russ Kennedy, Nasuni, p16

Twitter data breach worse than first thought - API attacks on the rise

A data breach in 2021 – which affected 5.4 million Twitter user accounts in the UK, Europe, and the USA - may have been worse than first reported. While the data was initially made available for sale on hacker forums and the dark web, it has since been made freely available for download.

The data was stolen via an API vulnerability which Twitter detected back in January 2022. That data, which includes private phone numbers and email addresses as well as scraped public information, was stolen by multiple bad actors – not just one actor as previously reported. These sorts of API attacks are expected to become more prominent because APIs represent a tempting target – essentially providing direct access to databases - for bad actors, considering the huge quantities of data they exchange.

As a result of the breach, users could see not just their Twitter accounts at risk, but also identity fraud for unauthorised online banking, shopping, and other social media platforms.

"The public disclosure of Twitter users' phone numbers enables an attacker to attempt to bypass 2FA or MFA, if enabled," said Joseph Carson, chief security scientist, Delinea. "Mobile phone numbers are just one step in the attack path to targeting users through MFA fatigue, but attackers may take the easy path and sell the data on to scammers to make themselves a bit of money."

Cybersecurity industry veteran Chad Loder claimed on Twitter that the breach was in fact more widespread, comprising tens of millions of Twitter records including account names, IDs, bios, screen names and personal phone numbers.

"I have just received evidence of a massive Twitter data breach affecting millions of Twitter accounts in EU and US. I have contacted a sample of the affected accounts and they confirmed that the breached data is accurate. This breach occurred no earlier than 2021," wrote Loder via Twitter.

Loder was suspended shortly after his Twitter post and has yet to be reinstated along with Donald Trump and Kanye West following Elon Musk's takeover in October.

Given that Meta was recently fined US$265 million by Ireland's Data Protection Commission for a data breach of 533 million Facebook users in 2021, it could only be a matter of time before Twitter faces its own penalties. While the breach is small fry in comparison to Meta's, it remains a significant proportion of Twitter's 200+ million active daily users.

Musk famously bought Twitter in a US$44 billion deal which, he admitted, significantly overvalued the platform, which is currently losing some US$4 million a day. Since the takeover, approximately half of Twitter's staff have been sacked in a money-saving exercise, which raises the following questions: "Can Twitter afford to pay a penalty for the breach?" and "In a time of such severe cost-cutting, will Twitter invest in more stringent security measures to protect data?"

As of the end of November, the answer is, apparently, yes. Twitter will bring end-to-end encryption (E2EE) to direct messages as part of Musk's vision for 'Twitter 2.0.' However, caution should not yet be thrown to the wind, according to Melissa Bischoping, director, endpoint security research, Tanium: "Despite whatever claims may be made about Twitter's secure messaging capabilities over the coming weeks, it would be advisable to use caution before entrusting any sensitive data considering the stability of what appears to be a rushed design." ■

IN DEPTH: Edging closer to climate neutral DCs p8-10

Aberdeen rolls out smart street lighting for remote monitoring

An intelligent street lighting project has been rolled out by Aberdeen City Council, unlocking sustainability and decarbonisation improvements across the city.

The Lighting Up Aberdeen project is part of a partnership with North and is helping the local authority create a greener future using energy-efficient lighting across the city. The project has seen a state-of-the-art IoT solution installed to manage and monitor more than 37,000 street lighting units remotely, enhancing the city's lighting provision, whilst simultaneously helping to create a greener and safer city for the people of Aberdeen.

With the new solution, there is no need for the manual process of checking lights, significantly reducing carbon emissions from travelling, while custom dimming profiles can be used to manage the level of energy required at any given time and automated fault reporting has allowed for more efficient maintenance. So far, Lighting Up Aberdeen has delivered considerable carbon reductions through a reduction in energy use, and, in turn, the council has seen significant savings across street lighting electricity bills.

"Aberdeen City Council is a forward-thinking local authority, using the capabilities of intelligent lighting to enrich its communities to become greener and safer," said Scott McEwan, acting CEO at North. "Working with local authorities across the UK, North is pioneering change through the power of smart technology and, collectively, we are creating a force for good that influences sustainability, health and economic success."

IT leaders optimistic in face of economic challenges

According to new research from Citrix, IT leaders are reserving an average of 30% of their budget for investments in innovation amid inflation uncertainty. Additionally, some 42% believed that managing the impact of inflation on their organisation would be the most significant challenge they will have to face in their career to date.

The study polled 250 IT leaders in UK businesses to explore the impact rising costs are having on IT spend, including which technology areas are being prioritised and where cost saving measures are being made.

"With budgets no longer spreading as far as they once did, IT leaders are understandably taking stock of their spend," said Mark Sweeney, regional vice president, UK&I, Citrix. "As a result, many have had to revisit existing digital transformation and innovation plans to work out which areas can be consolidated and which must remain a priority."

Some 55% of UK IT leaders are investing additional budget in internal innovation projects, such as improving digital workplace technology to support remote work, due to global inflation. Solutions that enhance the employee experience and aid retention were a priority for half of respondents, with the same amount also saying they are putting money into solutions to improve their organisation's security. Investing in technologies that support new ways in which their customers want to engage with them also ranked highly at 49%, as did driving cost efficiencies at 42%.

Despite the poor economic outlook, IT leaders are remaining optimistic about spend on technology. 76% said that their current tech budget would increase in the next 12 months, with 28% saying it would do so considerably.

Spends are, however, being re-examined and priorities re-considered within the current economic climate. 49% are streamlining workplace technologies as a cost saving measure, while revising hiring plans and reducing real estate footprint were also reported by 39% and 33% respectively. Overall, 32% were very concerned that current or future budget cuts due to inflation will have a negative impact on their company, and 30% said that this will have an impact on IT security within their organisation.

"It's positive to see investment in digital workplace technologies at the top of this list given the value these solutions bring to organisations, both through driving efficiencies and boosting productivity. With uncertain times ahead IT leaders must be strategic and think about where money is being spent and focus on the desired outcomes," said Sweeney.

Omdia: mobile and fixed broadband revenues to grow, but ARPU to decline

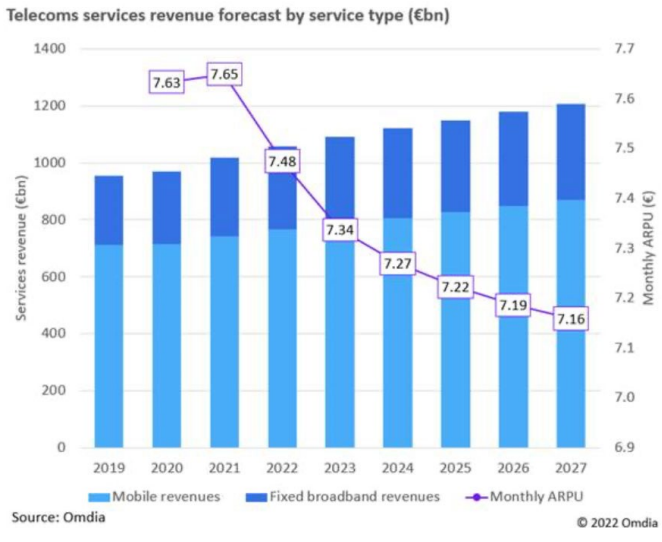
Total global telecoms revenues from mobile and fixed broadband services will grow 14% over 2022-2027 to reach €1.2 trillion according to the latest research from Omdia. However, monthly ARPU (average revenue per user) combined across both mobile and fixed broadband will fall by 4.2% from €7.48 in 2022 to €7.16 in 2027.

5G is no longer expected to be sufficient to offset ARPU decline in mobile markets because customers are unwilling to pay more for it. Unlimited data and video streaming services bundled exclusively on 5G contracts have had some success, but this only gives the industry the illusion of a 5G ARPU uplift.

In fixed broadband markets, the transition to fibre has had a net positive impact in most cases as the technology offers a much-needed step-change in home broadband quality of service on the back of the pandemic. However, markets with high fibre penetration are seeing a significant drop in ARPU such as France, Italy and China as competition intensifies and there isn't a clear monetisation path for fibre customers once they transitioned.

"People don't buy technology; they buy fun exciting new experiences. There is a misconception that operators should be reselling the technology they buy directly to customers, and it doesn't work," said Omdia research director Ronan de Renesse. "The network is the bedrock on which innovation and creativity can flourish like 4G and mobile apps. It is not just up to operators to solve the ARPU growth challenge but rather the rest of the digital services ecosystem. We will be discussing this issue as a matter of priority at the upcoming Network X event in Amsterdam."

Omdia forecasts that 5G will account for 5.9 billion subscriptions in 2027, equivalent to a population penetration of 70.9%. Consumer residential fixed broadband subscriptions delivered via fibre to the home will exceed 1 billion subscriptions by 2027, equivalent to a household penetration of 41.9%.



EDITORIAL:
Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Paul Keely, Urban Konrad, Russ Kennedy, Mark Oakton, Charlotte Bellett, Ray Hagen

ADVERTISING & PRODUCTION:
Sales: Kathy Moynihan
kathym@kadiumpublishing.com
Production: Karen Bailey
karenb@kadiumpublishing.com
Publishing director:
Kathy Moynihan
kathym@kadiumpublishing.com

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

ISSN: 2052–7373

ateb appoints Central Networks for in-house IT

Welsh housing association, ateb Group, has appointed Central Networks to support its in-house IT department with the provision of an outsourced help desk function and strategic consultancy.

Central is managing the social housing provider's help desk for its 130-strong workforce – receiving around 1,200 IT requests per year – enabling its digital team to focus on the tactical future of its technology estate.

"Against a backdrop of IT-resource challenges and economic uncertainty following the COVID-19 pandemic, we knew we needed to further bolster the support offered by our IT department," said Alex Jenkins, executive director for finance at ateb Group. "Working with Central means we have complete peace of mind that the daily tickets are being resolved, affording our head of digital systems the time and headspace to focus on the more strategic activities."

The contract covers first, second, and third-line support services, encompassing everything from general help desk support – troubleshooting and solving users' tech issues – through to device management and tactical decision-making.

"We're seeing many of our social housing clients requesting outsourced help desk support – as a way to reduce overheads and maximise internal resource," said John Blackburn, operations director and social housing specialist at Central. "We know flexibility is vital too, so it's available as short-term cover or a permanent part of the contract – bespoke to each organisation's needs at any given time."

"The Central team is a great sounding board and critical friend for us here at ateb," said Jenkins. "From penetration testing to cloud migration, they advise our digital team on key technology decisions, and also support our recruitment process with interview participation. They are a trusted pair of hands and go above and beyond to ensure we're getting the most from our investments."

Central has more than 30 years of experience within the IT and housing sectors. The company has previously worked with providers across the country, including Bron Afon, Eastlight Community Homes, Horton Housing, and Ongo Homes, to name a few. ■

Black Box to deliver UC from Gamma

Black Box has entered a new partnership with Gamma Communications plc (Gamma) to deliver connectivity and unified communications solutions from Gamma — including the company's market-leading SIP trunking services — as part of its consultation, design, implementation, and post-installation support services.

"By building Gamma's business communications into our service offering, we're now able to provide a full Unified Communications portfolio and meet evolving market needs in the UK as businesses migrate from PSTN/ISDN to SIP," said Matt Thomas, vice president and general manager EMEA, Black Box. "Gamma is an innovative company working at the leading edge of communications services, and our best-in-class services will work hand in glove to help customers overcome technical and operational challenges to realize the benefits of next-generation communications technologies."

Gamma has built a comprehensive portfolio of communications services with significant intellectual property, including cloud-based services such as SIP trunking and hosted PBX. Black Box will offer these services as part of its own managed service offering.

"Black Box is an exceptional partner for us because the company shares our vision of where the market is going and because it already has a strong customer base that will bolster our partner ecosystem," said Neil Taylor, head of partner sales at Gamma. "Black Box is a leading service provider that excels at wrapping its own services around those of partner companies. For companies in the UK, our partnership offers the best-in-class services essential to navigating business communications in the digital world." ■

Culina Group gains SD-WAN

Daisy Corporate Services has entered a new five-year partnership with Culina Group Limited for the provision of a future-proof, security-focused SD-WAN solution powered by Meraki.

"We've initiated this project in order to build upon our larger cloud first strategy. My goal is to build a robust, simplified and standard IT landscape for Culina Group," said Gary Donnelly, group CIO at Culina Group. "Using SD-WAN we can provide the flexibility, security and speed of deployment Culina Group needs. This is a significant step towards that goal and I look forward to Daisy's support in this over the next five years."

The Meraki SD-WAN solution will empower Culina Group with improved agility through a network that adapts to their current and future needs. The whole network can flex to their requirements without ever compromising security, allowing Culina Group to concentrate on innovation and customer experience.

"This new project will see us roll out SD-WAN across the Culina Group that focuses on security, with enhanced application control and performance. A flexible Enterprise Agreement will allow Culina Group to remain agile and expand critical infrastructure at pace. The new network supports the cloud first strategy, consolidates suppliers, and provides them with a strong foundation for future growth," said Chris London, head of sales specialists at Daisy Corporate Services. "Our status as one of only a small number of accredited Meraki Managed Server Providers in the UK meant that we were perfectly positioned as the ideal technology partner for this project. Beyond that, we have also delivered flexible commercial terms, delivering in-year savings to meet Culina Group's IT cost-saving targets." ■

Persistent joins forces with Software AG

Persistent Systems has announced a strategic partnership with Software AG to develop joint solutions to accelerate operational excellence by modernising applications and processes as well as moving data more easily across enterprises to unlock value. The partnership will address the challenges and opportunities that business leaders face as they transform their organisations.

Enterprises are increasingly faced with the imperative to deliver exceptional customer experiences by integrating applications and data that are deployed on-premises, on the cloud, and via hybrid platforms. Insightful decision-making requires access to organisational and third-party data. In addition, there is increased demand for applications and processes to become more automated, productive, and intelligent.

Persistent and Software AG will partner on joint go-to-market activities, including the development of industry solutions and accelerators for healthcare and life sciences; banking, financial services and insurance; and telecommunications. The newly created Professional Services Center of Excellence, which will be powered by a large talent base of Persistent-trained engineers, will bring the domain and technical strength needed to deliver these solutions to solve client business needs.

"The challenges facing organisations are getting more complex than ever: whether that's managing distributed workforces, disrupted supply chains or myriad trade regulations. And it all has to be done against a backdrop of an unpredictable economy," said Sanjay Brahmawar, CEO, Software AG. "These challenges won't completely go away, but what we can remove is some of the complexity of tackling them. We're looking forward to partnering with Persistent and its huge team of industry and solution experts, to help more customers simplify their connected worlds."

Persistent will leverage Software AG's products in its solution development around the following capabilities:

- Extending API-led integration to modernize connectivity between systems, things, applications, and partners leveraging webMethods
- Helping clients build and deploy scalable data pipelines and infrastructure using StreamSets
- Expanding Persistent's software product and platform engineering expertise to smart industrial products with Cumulocity
- Increasing client value in process consulting by applying ARIS in all automation opportunities
- Enabling innovation in enterprise IT with Alfabet, a leader in enterprise architecture management, planning tools, and portfolio management software ■

Velos IoT announces new senior staff

Velos IoT announces the appointment of two new senior staff members – Nicola Trudu as chief revenue officer and Frank Vernieuwe as chief technology officer.

The appointments are part of a plan to redefine the product portfolio and accelerate the integration of the three comprising businesses – JT IoT, Top Connect and NextM2M.

Nicola Trudu will be responsible for bringing the company's new vision into practice, while Frank Vernieuwe will look after the technology requirements. ■

Motorola Solutions to terminate ESN contract

Motorola Solutions has entered talks with the UK Home Office to terminate its contract for the country's Emergency Services Network (ESN), following a review of the future potential of its involvement in the project.

Motorola explained that it has taken a strategic decision to begin negotiations regarding an early exit from its ESN commitments. Motorola stated that it believed "the future service potential of the assets is limited."

As a result of the move, it has already recognised a fixed impairment loss of $147 million related to assets constructed and used in the deployment of the ESN contract.

Motorola and operator EE won a contract from the UK government in 2015 to provide 4G for the country's ESN and implement a new network to replace the existing two-way radio system run by Airwave, bought by Motorola in the same year. The upgrade was meant to be completed in 2020 but has been delayed for years due to escalating costs and numerous other issues. ■

Gartner: Scality #1 for Backup

Scality has been ranked #1 by Gartner for the Backup use case in the 2022 Gartner Critical Capabilities report for Distributed File Systems and Object Storage, among 18 storage vendors.

Scality was also recognised as a Leader in the 2022 Gartner Magic Quadrant for Distributed File Systems and Object Storage — for a seventh year in a row. Scality is also #2 in the Cloud-Native Applications use case, among 13 vendors, and ranked 4th and 6th in two other use cases — Archiving and Hybrid-Cloud Storage.

"We are honoured that Scality was recognised again in the Gartner Critical Capabilities," said Paul Speciale, CMO at Scality. "Ransomware attacks on backup data are on the rise, making backup and data protection among the most business-critical capabilities that IT teams provide. Scality's ranking as #1 in the Backup use case, we feel, reflects what our customers already know — that having an on-premises object storage solution for backup brings undeniable advantages, including freedom from lock-in, bulletproof data protection, and fast recovery." ■

Word on the web...

Mitigating infrastructure threats with SD-WAN

Craig Patterson, SVP of global channels, Aryaka

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

Network transformation: bringing efficiency and intelligence to multi-cloud with SD-WAN

Charlotte Bellett, head of solution design, Epsilon Telecommunications

Multi-cloud strategies have become widely accepted by enterprises, but the challenge is to maximise the potential of the cloud in their operations. Enterprises are increasingly choosing a multi-cloud strategy to avoid vendor lock-in and take advantage of best-of-breed solutions.

Enterprises are realising that the traditional approach to wide-area networks (WAN) is no longer compatible with today's multi-cloud environments.

Today, most enterprises will be considering a software-defined wide-area network (SD-WAN) as the next stage in their networking journey. SD-WAN emerged as a replacement to traditional WAN by providing simple, secure, and optimal connectivity between WAN endpoints, whether it be branch, data centre or cloud.

Moving to an SD-WAN environment can help improve application performance and security across multiple clouds, as well as gain greater network availability, reliability, and visibility, whilst lowering OPEX and CAPEX. Despite this, SD-WAN alone is not always the best path forward. Many enterprises do not realise the importance of the underlay network, which is vital for multi-cloud success.

Enterprises must be able to scale up or down with varying market demands. While public cloud services that run on the public internet provide this agility and scalability, they can be risky to rely on in case of outages and might not be adequately secure. A multi-cloud approach with SD-WAN can include a mixture of public clouds, as well as leveraging on dedicated ethernet or even a traditional MPLS network, to connect on-premises and to private clouds. This can help to ensure performance, security and 24/7 availability.

Many enterprises have the goal of removing some of their costly MPLS underlay network in favour of cheaper internet or hybrid internet/MPLS environments, which are also quicker to deploy. Others may be looking to get better performance and efficiency out of their existing WAN by considering the features that an SD-WAN overlay offers, such as application-driven routing, optimal path selection, and WAN optimisation.

SD-WAN makes it simple to utilise the network underlay resources in the most optimal manner for applications across multiple clouds. Enterprises can reduce overheads by delivering the connectivity, security, and optimisation from a single device.

SD-WAN can coexist with, and even enhance multi or hybrid cloud environments by integrating clouds and data centres as part of the SD-WAN, providing an intelligent networking solution with greater application visibility, manageability, and security.

SD-WAN is just the overlay for orchestrating the WAN. SD-WAN is a component of secure access service edge (SASE) architecture. Security Service Edge (SSE) is the security component of SASE architecture, providing a secure web gateway, cloud access security broker and zero trust network access that is best suited for distributed remote workers to have secure remote access to multi-cloud, on-prem services or software as a service (SaaS).

SD-WAN and SSE address different connectivity needs and complement each other to provide a SASE architecture to address both the remote user/end point and WAN requirements securely.

Enterprises should seek a service provider that can offer an end-to-end service, from initial design, to deployment, management, and evolution of the solution according to security and multi-cloud requirements. They should be able to provide an intelligent networking solution to connect sites over any combination of underlay technologies, be it internet, MPLS, LTE, public cloud, or private cloud.

Enterprises need a provider that can design the SD-WAN overlay solution in collaboration with them, to help analyse and understand their network requirements and provide an intelligent, multi-cloud-ready network to best meet their application needs.

The increased visibility that SD-WAN provides into the network helps enterprises to stay competitive, with superior network performance and security across different sites, clouds, and applications. However, it is the underlay and overlay network together which will deliver success for enterprises.

Multi-cloud doesn't have to be complex. The right solution and expertise can provide a solid foundation for the future, moving enterprises from basic cloud connectivity to advanced, end-to-end multi-cloud and SD-WAN network architecture. It should provide a fully managed and consistent multi-cloud design that is repeatable across any public cloud.

A solid intelligent networking solution should deliver advanced security to efficiently manage risk and protect data, as well as the scalability to easily scale up or down. Visibility is crucial for insights into performance and where data is stored, and enterprises should have full control with the ability to seamlessly move between clouds.

An intelligent network with underlay and overlay technologies working in collaboration can help take enterprise multi-cloud connectivity to the next level by providing improved insights, performance, and cloud capabilities, alongside added security for distributed workforces. With the right combination of automation and orchestration, enterprises can gain a solid foundation for long-term success. ■

Applying zero trust to an IoT network – essential or overkill?

Mark Oakton, CEO/CISO, Infosec Partners

According to IDC by 2025 there will be close to 42 billion IOT devices deployed by organisations connected to sensitive business-critical systems as more and more companies continue on a journey to full digital transformation. Whilst this trend is undoubtedly delivering significant commercial benefits, it has also created major challenges for IT teams who are tasked with building and maintaining the network infrastructure. Not least among them is the problem of ensuring that each time a new sensor is added they are not inadvertently providing tempting, targets for cyber criminals looking for easy back-door access to the entire network, systems and sensitive data.

Vulnerabilities in end-point devices can be the first port of call for most hackers. With many IoT devices located outside the network perimeter and regularly communicating in real-time with essential internal systems, the challenge for the security team is providing strong enough access control without negatively impacting functionality. This can lead to internal conflict between the IT team and the CISO, particularly for organisations that have adopted the zero-trust approach to network security and who will have some different priorities.

Zero-trust is based on the principle 'Never trust – Always verify' which applies equally to people as well as devices. A term coined about eight years ago by John Kindervag, an analyst at Forrester, it essentially requires a radical change of mindset when it comes to allowing access to networks and its resources. Traditionally users' credentials have been checked at the network edge when, if verified, are allowed largely unfettered access to any applications, systems and data. Zero trust means that the identity of every user or device must be constantly verified not just at the network edge but before accessing specific micro segments of the network for every session.

From a security perspective, a zero-trust approach offers an ideal framework to prevent cross-contamination and data leakage between critical applications. If somehow there has been a successful breach in one segment it is contained so that it cannot allow access to the rest of the network, making it much harder for threats such as DDoS and ransomware attacks to succeed.

From the IT team's perspective, zero-trust can be seen as just adding more workload for the already stretched (human) resources at their disposal. It means that all endpoints including IoT devices need to be continually monitored, checked and updated in line with changes to the network. In the past it might have been okay to check and re-configure a firewall or update IDS rules once or twice a year, but with multiple IoT devices in multiple locations performing multiple tasks possibly using different communications protocols, the zero-trust approach can be much more onerous if handled internally, requiring a more rigorous process of ongoing monitoring.

Ultimately a successful network security strategy relies on being able to detect suspect activity and breaches as early as possible in order to prevent a threat from escalating into a major, potentially catastrophic, incident. For many organisations the problem is not in the lack of information about what is happening on the network at any given time. Most, if not all organisations will have at least a firewall and probably an IDS or IPS and even a SIEM appliance providing alerts with real-time and historic traffic data to help identify the source and target of any malicious activity. However, in reality the signs can be often missed by security teams just through pressure of work.

The recent growth in the deployment of IoT devices has not just increased the attack surface available to hackers but has also massively increased the scale of the operation needed to protect the network.

Clearly, deciding whether to implement a zero-trust approach is an important decision for any organisation, particularly those that have made the move to a cloud-only or hybrid model as part of a digital transformation strategy. With many applications now residing in the cloud and accessed from potentially remote locations outside of the LAN, the decision has become even more mind-blowing for the usually non-tech-savvy c-suite.

This means that bringing in specialist third-party help to navigate all the cost/benefit issues is probably going to be needed to ensure the right decision is made not just in principle but in selecting the best vendor/partner from the list of what Gartner call Zero Trust Network Access (ZTNA) solutions. ZTNA is now the most common format for deploying zero trust policies and the good news is that organisations have a plethora of vendor options to choose from.

The not so good news is that while all are based on the same basic principle of suspect everyone/trust no-one, when it comes to controlling who is allowed access to the network, they all offer the same basic set of features but with a slightly different approach and price points.

However, one important common feature is that the market leading systems are delivered predominantly as-a-service, which makes selecting the right service provider a critical factor in the process, not just to ensure that the chosen solution meets all the operational requirements but can be constantly monitored and updated by a team of highly qualified and experienced cyber experts. ■

SD-WAN: the benefits, the challenges

Urban Konrad, senior manager systems engineering Switzerland & Austria, Palo Alto Networks

The COVID-19 pandemic has changed the way companies work forever. The number of remote employees who need to access corporate services, applications, and data from home has increased in no time at all. However, current monitoring tools do not provide visibility into all network segments in the service delivery path and require additional agents or appliances to be deployed in the infrastructure. Different solutions provide incomplete and inconsistent security for employees on-site, in branch offices and at other locations. This can result in more complexity and management effort.

Legacy technologies have severely limited the ability to efficiently manage growing traffic and security threats. Enterprises have been forced to deploy multiple products to meet changing business needs, including firewall, SWG, CASB, and SD-WAN. Supporting remote work has only made this more difficult.

Enterprises have turned to SD-WAN to reduce costs, improve the user experience and strengthen cloud connectivity. However, SD-WAN also brings with it many challenges, such as lack of security and high complexity. In addition, network performance is less reliable because companies use the congested internet as a WAN middle mile, usually without SLAs. Companies then turn to multiple vendors or service providers to solve performance issues, which drives up costs and reduces control and visibility. A better option is a subscription-based SD-WAN solution for next-generation firewalls.

With the right SD-WAN solution, an organisation can centralise control, management and visibility of branch office connectivity to the cloud. IT and security teams can protect branch offices from all types of attacks by leveraging rich data protection, security data, automation, threat intelligence, and machine learning. Here lies the potential for a huge improvement in cybersecurity.

Using a subscription-based SD-WAN solution to activate next-generation firewalls under the SASE umbrella is a contemporary approach. This enables easy adoption of an end-to-end SD-WAN architecture with natively integrated security and connectivity. It supports multiple deployment options, including mesh, hub-and-spoke, and cloud-based deployments.

An SD-WAN solution of this kind allows organisations to easily adopt an end-to-end architecture with natively integrated, best-in-class security and connectivity. Using branch-to-branch, hub-and-spoke and/or full-mesh topologies, they can optimise the performance of their entire network. This improves latency and reliability, improving the user experience in branch offices.

Regardless of the deployment model, tight integration enables the management of security and SD-WAN from a single, intuitive interface. This makes it possible to measure and monitor communication paths and to move sessions in order to ensure the best user experience in the respective branch office. Organisations can begin securely routing branch office traffic to their cloud applications and between other locations. With the help of profiles for path quality, SaaS application path monitoring, error correction and traffic distribution, companies can optimally operate any application in the cloud.

SD branch is a new approach that influences the way companies shape their networks. SD-Branch uses the principles of SD-WAN to simplify the infrastructure required in branch offices to support an IT system. Implementing SD branch technology can reduce potential threats that IoT devices could pose to a branch office network. As the expansion of IoT environments also leads to more data being transferred to a cloud environment, SaaS security is becoming increasingly important for protection against data loss and malware.

A next-generation SD-WAN solution provides standard SD branch features such as zero-touch provisioning and network visibility. Automation, lower total cost of ownership, higher application performance, and a variety of security and network services from the cloud also supports the implementation of the SD branch approach.

Whichever path companies take, cybersecurity will remain a recurring theme. A SASE solution must provide consistent security services and access to all types of cloud applications delivered through a common framework. By replacing multiple stand-alone products with a cloud-based SASE solution, organisations can reduce complexity, support remote workers, deploy and scale branch offices faster, and enforce consistent security. In addition, considerable resources can be saved.

The interaction of all SASE elements provides mobile users, branch offices and retail locations with reliable connectivity and consistent security no matter where they are and what device they are using. Now, organisations can quickly identify users, devices, and endpoints, apply their network access and security policies, and securely connect users to their applications and data in a cloud or mobile environment. At the same time, the security of enterprise environments with multiple branches and clouds is ensured.

SASE also enables companies to significantly reduce investment costs and the operating costs associated with deploying large-scale security and networks. More importantly, it accelerates deployment and shortens the time to provide protection by eliminating the need for traditional IT infrastructure. Above all, SASE provides a holistic overview of the network in order to better protect it. SASE simplifies network complexity and management by consolidating SD-WAN and other network infrastructures into a single cloud-based platform. This allows organisations to apply consistent security measures to stop cyberattacks. ■

Simplifying the transition to 100G and 400G

Ray Hagen, global product line manager, ProLabs

Expansion in the access network is a major trend in the UK, and indeed globally. GPON type services are seeing a lot of growth, primarily driven by the pandemic; remote working, home-schooling, and other factors. Now that we're post-pandemic, we're seeing continued growth driven by governments investing in broadband infrastructure, which opens a whole new world of possibilities.

In the past, the majority of access network technologies were 10G optical signals. Now they're being upgraded to 100G, a tenfold increase, or even 400G in some cases – it's quite the change.

For us, **100G is the new 10G**. 10G deployments typically feature a single optical line, P2P type technology, which is very flexible in how it could be deployed; up to 80km and at industrial temperatures. But with increased data rates, there are physical limitations. As a result, 100G is not nearly as flexible to deploy due to multiplexing which is the requirement for multiple optical lines on a single fiber.

Rolling out 400G is also complex. Different techniques are used to achieve 400G, like pulse amplitude modulation (PAM4) technology. Optical signals modulated with PAM4 are not backwards interoperable with legacy technology, or non-return to zero (NRZ). Careful planning is required on behalf of service providers and data centre operators to ensure comprehension on technology implementation.

At ProLabs, we spend a lot of time helping our customers understand amplifications and the complexities involved in 100G and 400G. In some cases, four 100G transceivers can be aggregated into a 400G port, but there's also 100G NRZ transceivers which can't be aggregated for 400G; that makes things more expensive for the customer, who must maintain different inventory points for different transceiver types.

Additionally, there have been considerable problems in acquiring equipment: many service providers and data centres have been waiting for more than a year to get their 400G equipment. However, things have started to settle, and clients are receiving shipment confirmations and can begin planning their rollouts.

The transition to 100G and 400G is unstoppable. Customers are migrating to 400G to meet the increased demand for bandwidth. The pandemic really set the stage for the streaming revolution in the sense that it is no longer a revolution; it is now simply a part of daily life. As a result, service providers must have enough bandwidth to support this, while data centre operators need to ensure their networks can handle such vast volumes.

Right now, there are two distinct 100G user groups: service providers and data centres. Enterprise networks aren't quite there yet; in recent years, they've been hindered by out-of-office employees and have had to rely on upgrading their VPN concentrators to accommodate remote working. I believe that in 2023, we'll see a greater return of working in office, which will change things for enterprise - we'll probably see more investment in the local area network.

To date, data centres have been the primary application for 400G, which has been performing data centre interconnects over the last year. Going forward, we expect to see 400G being used from the core outward, on the data centre floor, where it will continue to aggregate 100G from individual cabinets and servers back to a 400G core. In 2023, core network service providers will most likely join data centres in deploying 400G. We also anticipate that 400G will be deployed for long haul networks and IT service providers in the coming year.

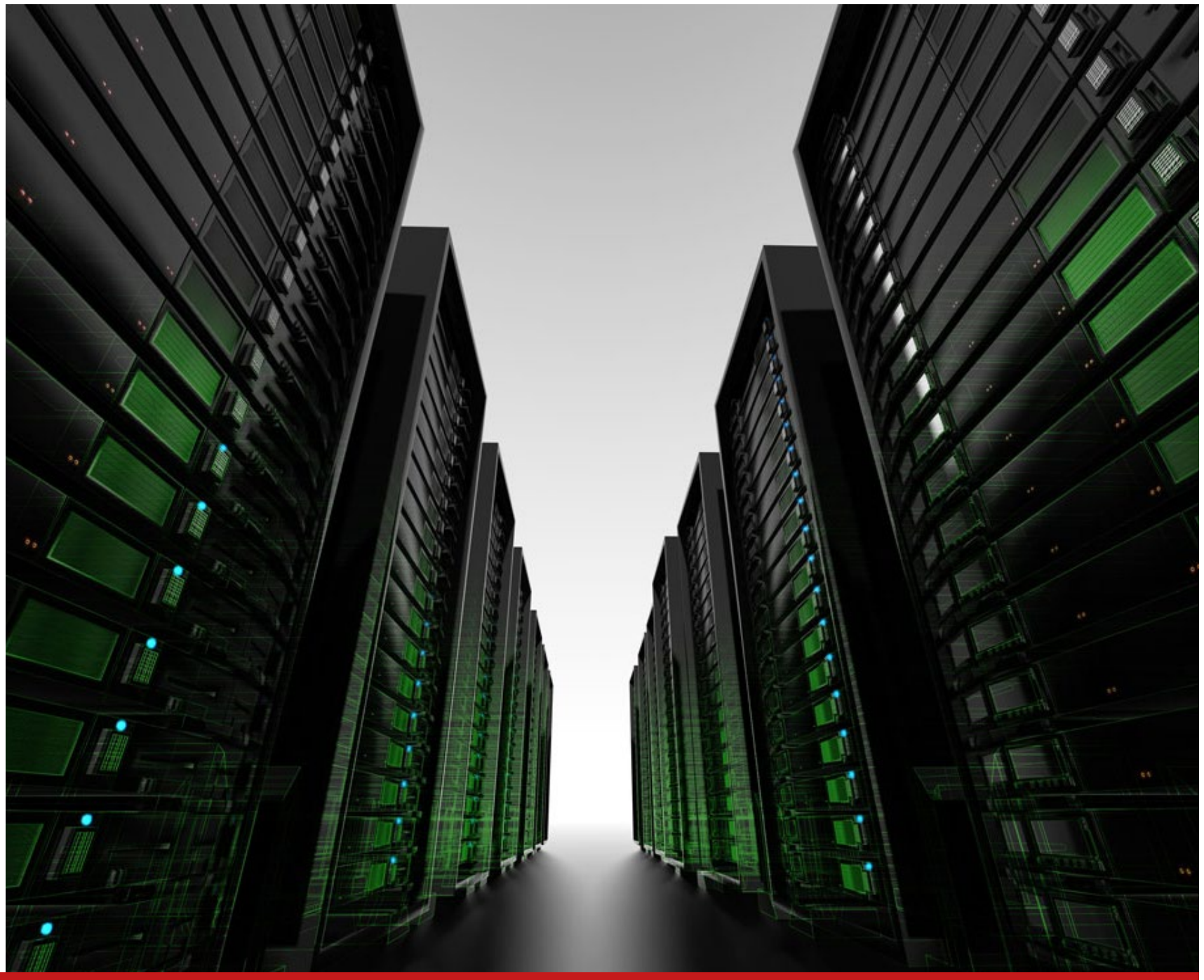
To help our customers in navigating these upgrades, we take on a consulting role, advising on the most cost-effective way to improve their network deployments. In recent years, inventory has been a significant barrier for those looking to upgrade their networks. At ProLabs, we always keep a large stock of inventory on hand; we can ship same-day or next-day, so that our customers don't have to worry about it.

We offer transceiver-based solutions to the challenges faced in network upgrades. Our comprehensive line card includes both 100G and 400G transceivers for every network application. Everything from run rate 100G optics for short reach applications to 400G coherent optics used in transport applications.

Our approach has resulted to the launch of innovative products for specific network needs. For example, 100G over a single fibre, or a fully passive wavelength division multiplexing of 100G up to 40km and a EDFA and MUX in one package to transport 100G DWDM up to 120km over single mode fibre. We also assist our customers in navigating the migration from NRZ to PAM4. The shift to PAM4 is a generational change in networking that requires thoughtful planning to protect the life of existing network assets.

We are unique in how we go to market and provide a 100% lifetime warranty. In our labs in the UK and the US, we test every transceiver in its intended environment before it ships. That helps us maintain a very high level of quality, and we provide customers with a Data Traveler System™ (DTS) certificate, which shows how the transceiver tested before shipping.

100G is taking the place of 10G at many of our customers' networks. In turn, that increased bandwidth is going to drive a need for 400G. We're poised to provide validated, cost-effective solutions at every step. ■



In search of the climate neutral data centre

Data centres play an essential role in our increasingly digital world; however, they also consume up to 3% of global power production. This is only going to rise in line with exponential data generation. Amy Saunders explores how UK data centres can aim for climate neutrality

Data centres, whether real or virtual, provide an essential service as centralised locations for processing organisations' IT operations and equipment to store, process and disseminate data.

The post-pandemic market

In the UK, data centre market demand has boomed since the onset of the COVID-19 pandemic. Some capex was delayed by the pandemic, with contracts remaining incomplete until social distancing rules ended, however, that time is now behind us.

Research and Markets reports that there were more than 200 third-party data centres in the UK with almost 1 million square metres of raised floor space and more than 1,000MW of data centre customer power (DCCP) at the end of 2021. Data centre space is expanding by existing data centre providers at more than 50,000 square metres annually, mainly within the London and Inner M25 and Slough areas. An additional 20,000 square metres of data centre space is being added to the UK market annually by regional data centre providers. Investment in data centre capacity in lower cost regions will be a key trend going forward. UK data centre revenue growth of 36% is expected over 2021-2025, while data centre space and power are forecast to grow by 26% and 29% over the same period.

The London data centre market represents around 80% of the UK total. CBRE reports that in the first quarter of 2022, there was 17MW of capacity take-up and 46MW of new supply. Demand from hyperscalers remained strong despite considerable market constraints, and is expected to accelerate in the second half of 2022, particularly in London, with

wholesale lettings to single tenants, usually hyperscalers, dominating the market.

"The UK and Ireland data centre sector continues to experience year-on-year growth, with London being home to the world's second largest hyperscaler market," said Billy Durie, global sector head for data centres at Aggreko. "However, with the energy consumption of these facilities now rising in line with this market expansion, ensuring that this growth takes place in a sustainable manner is more important than ever."

Mordor Intelligence reports that the UK is home to more than 5.5 million businesses that rely on cloud services, which, when combined with non-business IT cloud needs, could potentially lead to 7,446kWh power use by data centres annually by 2025, more than the total renewable generation standard. To maintain renewable generation standards, the UK government issued a regulation which requires all companies with 250+ employees to report their power usage under the Energy Savings Opportunity Scheme (ESOS). This is expected to drive the demand for energy-efficient data centres.

Climate neutrality

Data centres are estimated to consume anywhere from 1-3% of a nation's total power consumption.

"Fortunately, the gravity of this situation is being recognised, with data centre operators and trade associations agreeing to make data centres climate neutral by 2030 as part of the Climate Neutral Data Centre Pact," said Durie. "It would be fair to say that sustainability is now a top priority for those operating in this region."

Indeed, many have committed to becoming climate neutral by 2030, and as of July 2022, 74 data centre operators and 23 associations have signed up to the Climate Neutral Data Centre Pact, which requires:

- Increase and measure energy efficiency - European data centres and server rooms shall meet a high standard for energy efficiency through aggressive power use effectiveness (PUE) targets. By 1 January 2025 new data centres operating at full capacity in cool climates will meet an annual PUE target of 1.3, or 1.4 for new data centres operating at full capacity in warm climates. Existing data centres will achieve these same targets by 1 January 2030.
- Clean energy - Carbon neutral data centres should be powered by 75% renewable energy by 31 December 2025 and 100% by 31 December 2030.
- Water efficiency - Water use is to be reduced to a minimum by the application of a location and source sensitive water usage effectiveness target (WUE). By 1 January 2025, new data centres in cool climates must be a maximum WUE of 0.4L/kWh in areas with water stress. By 31 December 2040, existing data centres that replace a cooling system should meet the same target.
- Circular economy - Operators must apply circular economy practises to repair and recycle servers, as well as reusing waste heat where possible.
- Circular energy - The reuse of data centre heat presents an opportunity for energy conservation that can fit specific circumstances. Data centre operators will explore possibilities to interconnect with district heating systems and other users of heat to determine if opportunities to feed captured heat from new data centres into nearby systems are practical, environmentally sound and cost effective.

Legacy data centres represent one of the biggest challenges; those built 10 or more years ago consume huge amounts of energy and will require heavy investment in the years to come for decarbonisation. For newer and upcoming data centres, however, there are many features that can be incorporated from the planning stages to produce a more environmentally friendly facility. Immersion cooling, the application of artificial intelligence for workload management, and sourcing renewable materials for construction are just the tip of the iceberg. As well as proving positive for the environment, such measures lower opex for the lifetime of the data centre.

Sustainability: power is key

Sustainability has been important for all those in the UK's value chain for some time now, according to David Watkins, solutions director for VIRTUS: "For over a decade we have recognised the need to produce more efficient data centres, actively lowering PUE and WUE with innovative designs. These ongoing efficiency efforts have ensured that the industry has already made great strides to mitigate their impact on the environment."

Simon Brady, head of data optimisation at Vertiv, agrees: "Sustainability is a priority for all data centre providers in the UK. With the growth of internet 2.0, IoT, AI and everything as a service, the industry's energy usage is only going to increase. This means we MUST put sustainability at the core of our business model."

However, unique challenges arise from creating greener data centres. "While data centres don't generate waste or products like other industries, this high energy and water-use sector faces unprecedented demand for sustainability measures and efficient facilities. The most forward-looking providers are committed to delivering a 'cradle to grave' green strategy, where environmental ambitions are built into every step of data centre design, construction and maintenance," said Watkins.

Durie agrees, highlighting two key aspects for consideration: "operational emissions, and embodied emissions. The former often dominates this conversation, and concerns reducing the carbon footprint of day-to-day operation through limiting water and energy usage or making use of renewable sources. However, it is also important to address the issue of embodied emissions – all carbon expended during the construction of a new facility. Given that new data centres continue to be constructed all the time, only through assuaging both these concerns can the sector become more sustainable."

There are a range of technologies and solutions in play that can help reduce emissions from data centres. "Better thermal management of legacy sites by removing high-energy consumption mechanical cooling systems could make a difference. The main obstacle is fear of change and how that will impact availability and uptime," said Brady.

"Power used for cooling accounts for much of the emissions from data centres," said Watkins. "We have deployed well-established technology developments to tackle power usage such as liquid, evaporative, fresh air and adiabatic cooling. Direct chip liquid cooling can offer some of the lowest PUE possible as the temperature at which they operate means that no mechanical or adiabatic cooling would be required. Renewable carbon-zero energy is also an important part of the strategy to reduce carbon emissions."

Durie reiterated that power, often supplied by diesel gensets, is a key source of carbon emissions during data centre construction. "The main aspect to consider here is right sizing – opting for solutions that do not exceed the power demands of the site," he explained. "This can be difficult due to the varying load demands of an active construction site, but can be achieved through a load on demand system, where several smaller generators are favoured over a singular large unit, scaling up or down as required. This leads to a significant reduction in fuel consumption, and in turn carbon emissions. By taking this one step further and switching to a hybrid and load on demand system of two 60kVA Stage V generators, a typical site with power requirements of 200kVA can achieve a 50% reduction in CO2 emissions and fuel consumption."

Going green in the UK

When it comes to creating climate neutral data centres, there are a wealth of options.

The first step is the move away from fossil fuels. "Data centres are particularly well placed to benefit from renewable energy sources due to their stable power consumption," explained Watkins. "VIRTUS was the first UK provider to commit to using 100% carbon-zero energy – powering its sites solely with truly renewable energy from wind, solar and tidal sources since 2012. By doing this, VIRTUS saves around 45,000,000 tonnes of CO2 every year, enough to fill Wembley stadium five times over."

Hydrotreated vegetable oil is proving a popular alternative fuel within the UK: "instead of making use of diesel in gensets, data centres can substitute this fuel for hydrotreated vegetable oil, a greener alternative that can facilitate up to a 90% reduction in carbon dioxide (CO2) emissions and a 15-25% reduction in nitrous oxides (NOx) and particulate matter (PM)," said Durie.

Watkins agrees that "the use of hydrotreated vegetable oil instead of diesel in generators has the potential to reduce carbon emissions by up to 90% - as well as eliminating sulphur dioxide emissions and reducing harmful nitrogen oxides."

Other technological developments in areas such as fuel cells are continuing at a pace "and whilst they're not viable right now, if they can perform at scale, they might present a compelling option for future green data centre power," added Watkins.

The application of other renewable energies, however, is more complex: "some data centres are investing in onsite generation of lower carbon sources of energy, but today the power density is not available, partly because wind and solar require a lot of space which isn't conducive to the very high density of power a data centre needs," said Brady. "UPS technologies that offer dynamic grid support through battery backup are possibly the way forward. To green data centre power consumption, the energy suppliers need to add more low carbon power to the grid. The higher the percentage of lower carbon sources, the greener everyone's power consumption will be."

A sustainable future

To continue to strive for the most sustainable data centres, operators must consider a green design from the outset.

"We need to build sustainability into design, right through to end of life and existing owners/operators should invest more in upgrading legacy sites to make better use of the energy they consume. Given the current increases in energy costs the ROI for such projects can now be measured in months rather than years," said Brady. "ESG must continue to be a focus during everyday operations and when technology refreshes happen."

"As the UK and Ireland data centre market continues to grow, decarbonising both day-to-day operations and the construction of new facilities will be key to achieving truly green data centres," added Durie. "Through incorporating technologies such as Stage V generators and HVO and taking a more granular approach to all aspects of carbon emissions, the sector will be able to achieve its goal of carbon neutrality by 2030."

With data centres very much a staple of modern-day life, the push towards sustainability is a must.

"One of the most efficient ways to deliver a unit of computing (energy per compute unit) is to put it in a large, modern, advanced data centre on a cloud platform. These data centres are also far more energy efficient in comparison to previous models of computing," said Watkins.

Moreover, at the consumer end of the scale, common data service uses like online shopping and remote working have delivered sustainability benefits throughout the chain, reducing the CO2 emissions associated with travel. Thus, while the data centre segment may have a way to go yet before achieving climate neutrality, the impact of data centre services is already delivering widespread green benefits throughout the UK, and indeed, the world. ■

Park Holidays modernises to continue M&A expansion

Park Holidays UK is one of the largest operators in the country, offering static caravan and lodge holidays, 'glamping' and holiday home ownership in locations spanning Cornwall to Scotland. Park Holidays UK has grown organically and through numerous acquisitions and now includes 54 locations nationwide.

A lifetime of upgrades

A long-term user of VDI and thin client technology, Park Holidays first deployed a combined IGEL and Citrix solution ten years ago to address bandwidth issues at some sites and standardization of desktops. The solution enabled Park Holidays to move away from unreliable and high maintenance PCs so that support could be simplified, and endpoint deployment, configuration and management made faster and easier.

In recent years, Park Holidays has completely modernized its entire IT environment by investing in new desktops, server virtualization, SAN storage as well as a MPLS-based Wide Area Network to interconnect all the holiday park sites.

In 2019, the business also shifted IT applications and its Avaya phone system to the cloud – running in Microsoft Azure. Furthermore, Microsoft 365 and Dynamics 365 Business Central were implemented, with Elite Parks software – built on Dynamics 365 – used as the company's ERP system.

Supporting ambitious M&A growth

To meet Park Holidays' ever-growing needs, earlier this year IGEL implemented a company-wide strategic solution to support an ambitious mergers and acquisitions (M&A) growth strategy, offer access to applications running in the cloud and allow the introduction of video conferencing for all staff leveraging Microsoft Teams.

"We've taken a 'cookie cutter' approach to the desktop. In other words, we have one uniform system across the company so that when new parks are acquired, we just drop in Citrix and IGEL to rapidly deploy desktop services," said Michael Procyshyn, Park Holiday UK's IT director. "It allows us to scale up our infrastructure and systems quickly and cost effectively, with the joint solution a real enabler for growth."

Indeed, the Citrix and IGEL OS-powered endpoints deliver a range of benefits to Park Holidays.

"When we last reviewed our desktop approach, we concluded that moving away from IGEL's technology to laptops or PCs would be cost prohibitive," said Procyshyn. "IGEL and Citrix helps our rapid expansion plans because we know we can deploy endpoints simply and painlessly."

Security has been enhanced with server-based and centrally controlled security. IGEL endpoints are locked down to the extent that staff can't amend the master desktop image or load in applications locally.

Native support for cloud-based applications has been implemented via IGEL OS and IGEL hardware, which support VDI and DaaS applications. This is key as Park Holidays UK has shifted wholesale to a Microsoft-based cloud environment. IGEL solutions are supplied by IGEL Velocity Partner, Ventrus Networks.

Meanwhile, staff onboarding, the integration of new hires into the organisation, can now be achieved faster, supported by a combination of cloud-based applications. Citrix and IGEL OS-powered endpoints – managed using IGEL UMS - mean that Park Holidays UK can quickly and easily amalgamate acquired businesses.

"We know of one competitor who took two years to integrate some of their acquisitions," said Procyshyn. "When we purchased Bridge Leisure, it took us just four weeks to migrate the nine sites over and roll out access to our systems whilst onboarding staff."

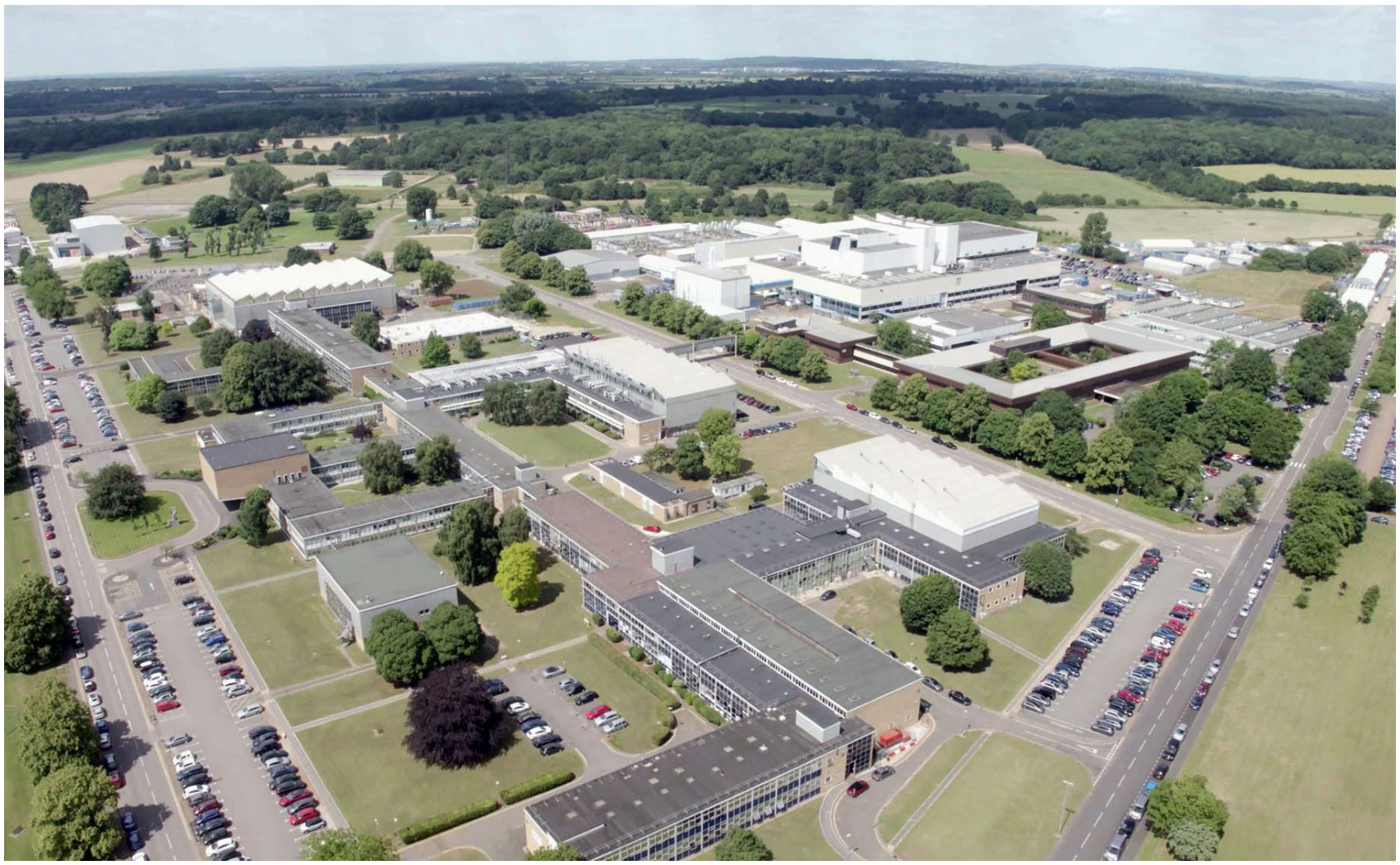
Staff can now work easily across Park Holidays' sites with the new standardized desktop applications accessed via Citric, enabling access to corporate applications and their own folders and files. Operationally this makes it much easier for Park Holidays UK to resource its business from a staffing perspective, especially during peak holiday times.

Additionally, management has been simplified and reduced in cost thanks to the IGEL Universal Management Suite (UMS), which is now is used to remotely control the whole distributed environment. Just six technical staff are needed to manage an IGEL estate of 500 endpoints and provide technical support to all employees who use them day to day.

Going forwards, Microsoft Teams will be installed to enable video conferencing capabilities, utilizing the native power of IGEL endpoints running IGEL OS. Evaluation trails are currently underway, and some devices are expected to be updated.

"One of the key strengths of Park Holidays UK is our IT. Our networking, infrastructure and applications are robust, reliable and all the same; we don't dual run anything as this just adds complexity," said Procyshyn.

Commenting on the project, Simon Townsend, IGEL's chief marketing officer, said: "At first glance, Park Holidays UK might appear to be a simple caravan related business, but it's actually a diverse organization. They run a large hotel chain – selling holidays in lodges and caravans – but it's also a restaurant and pub company, and a property and maintenance firm given it manages the parks and the holiday homes purchased by owners," said Townsend. "So, it has a variety of staff who all need simple access to corporate IT systems and the Internet. Citrix and IGEL enables this, resulting in lower desktop TCO and a great end-user experience." ■



UKAEA gains new flexibility with Cinos

The UK Atomic Energy Authority (UKAEA) carries out fusion energy research on behalf of the UK Government. Its mission is to lead the delivery of sustainable fusion energy.

Fusion energy has great potential to deliver safe, sustainable, low carbon energy for generations to come. Described as the ultimate energy source, it is based on the same processes that power the sun and stars. The UK is leading the way and has a huge opportunity to become a global exporter of fusion technology.

Unrealised cloud benefits

The UKAEA had previously updated its telephony system to transition away from a legacy analogue phone line system, thus it already had a voice over internet protocol (VoIP) service in place. However, the organisation was experiencing some challenges realising the full benefits from the cloud service, which was managed by a previous supplier.

Used by all staff across its main site in Culham, South Oxfordshire and remote site in Rotherham, the UKAEA needed a system that could support collaboration, enable staff to work remotely and aid innovation throughout the business.

"The challenge with our previous cloud-based solution was that it wasn't very flexible. We needed a much more agile service to enable our staff to collaborate more effectively with the hybrid working approach that we implemented during the COVID-19 lockdowns," said Andrew Hynes, head of CODAS and IT at UKAEA. "Video conferencing and collaboration tools such as Microsoft Teams and Zoom are a big part of how we collaborate as an organisation, but we were missing functionality that would allow us to integrate softphones. It was important to unify our services and enable phone lines to be forwarded to mobile devices and computers, while being able to integrate with Microsoft Teams."

Unified communications

In June 2021, UKAEA awarded a contract to Cinos to deliver a secure, reliable and robust unified communications service. Deploying its Cisco Powered, sovereign UC service based within the Cinos Cloud, Cinos migrated 2,000 users and handsets to the new system across both UKAEA sites.

"Cinos guided us during the implementation and created a very structured process from start to finish," said Hynes. "As the project was delivered remotely, we set up a Microsoft Teams site to aid the collaboration process and share documents. The technical expertise demonstrated by the Cinos team meant that we were able to easily manage the migration from the previous provider and deliver the project in a timely fashion. With a lot of careful planning and testing, it was seamless."

In line with UKAEA's requirements and as part of the implementation process, Cinos rolled out Cisco Jabber softphones to enable integration with Microsoft Teams. This allows landline or mobile phone calls to be made and taken through the application, functionality that wasn't available previously. It introduced the reliability and robustness of Cinos' telephony services to Microsoft Teams.

"It was really important to us that the new solution would enable us to integrate Cisco telephony with Microsoft Teams and unify our services," said Hynes. "Cisco Jabber has given us the best of both worlds as our staff are now using Jabber more than they are their desk phones, so the level of engagement has been high."

Maximising functionality

Working in partnership with Cinos, UKAEA has been able to maximise functionality and put in place a flexible UC system that is robust and enables collaboration as well as giving the organisation room to grow and innovate in the future.

Being able to access the system at all times has provided UKAEA with a trusted platform for uninterrupted communications. Benefitting from Cinos' expertise in full resilience and critical communications solutions, UKAEA also deployed a built-in internal emergency line, instilling confidence that emergency calls would be routed quickly and efficiently.

By utilising Cisco Jabber, telephone services were unified under one solution giving increased control, allowing users to select a device of choice to answer calls on. This ability complemented flexible working, providing access to the system irrespective of geographical location. Moreover, as a result of being able to reroute calls between devices, UKAEA was able to retain its existing investment in handsets, without the need to purchase additional devices and therefore avoiding additional costs.

"The support that we've received from Cinos throughout and post go-live has been fantastic. Not only did they almost immediately answer any queries we may have had, they also took ownership and responsibility of any communication with our previous supplier. This meant the implementation was seamless and ensured that we felt confident throughout the process," said Hynes. ■

Overcoming the challenges to IoT and OT security

With billions of devices becoming connected as the Internet of Things (IoT) expands its reach across the globe, the security of these devices must be considered. Paul Keely, chief cloud officer at Open Systems, explains the moves enterprises can take to safeguard their systems

Enterprises have truly embraced the Internet of Things (IoT), with businesses the world over deploying ever more of these connected devices. From improving workplace efficiency and promoting employee morale, to increasing the performance and reliability of manufacturing operations, businesses are projected to spend over US$400 billion on IoT worldwide by 2025.

Despite their benefits however, this proliferation of IoT devices has also greatly expanded corporate attack surfaces, giving bad actors more potential points of entry into corporate networks. Compounding this, these devices often have inherent weaknesses, which cybercriminals can exploit to compromise them. A single compromised IoT device is all criminals need to breach a network and then move about laterally to find valuable data to exfiltrate.

Obviously, securing these smart devices should be a top priority given their vulnerabilities. The sad truth, however, is that few companies put the same effort into protecting their IoT devices as they do their laptops, servers and other IT assets. To understand why, it's important to first understand the two broad categories of connected devices and their unique security issues.

IoT security issues

In the business world, IoT typically refers to devices deployed in office spaces to make them more comfortable for employees and to improve workplace efficiency. Applications run the gamut; from smart juicing machines that order their own fruit, to conference room sensors that indicate if they're in use or empty.

While undeniably useful, such IoT applications are not mission critical. This fact, combined with how easily these devices are to install, means deployments are typically handled by facilities teams – and often by individual employees – rather than IT. It is this lack of IT involvement that leads to serious security challenges.

The problems begin immediately because the default passwords of these devices are rarely changed during installation, despite the best intentions of the facilities staff deploying them.

Additionally, most IT organisations do not know the number or types of IoT devices that have been deployed throughout their enterprise. This lack of visibility makes proper patch management extremely difficult and means that patches and firmware updates are rarely if ever implemented.

Complicating things further, many of these IoT devices may no longer be supported and many vendors may have gone out of business. Despite this however, the devices often remain active, connected, and become increasingly vulnerable points of entry for bad actors.

The IoT threat landscape is also increasingly dire now that Trickbot, a malware targeting computers and IT systems, now affects IoT devices as well. Trickbot has compromised IoT devices in command-and-control (C2) attacks, using them to attempt lateral movement to access to a network with more critical data.

OT means business

Operational Technology (OT) is the other category of connected devices and is sometimes referred to as Industrial IoT (IIoT). As the name suggests, OT is employed by companies in the monitoring and controlling of the equipment and processes that are key to their business. Unlike IoT, OT is often used in business-critical applications.

Predictive maintenance is a popular OT application, used to identify signs of failure in critical equipment so that maintenance can be performed to prevent a breakdown. A good example is a connected sensor that detects increased vibrations indicating the imminent failure of turbines or other high-speed rotating parts in a critical piece of machinery.

Given their importance and significant cost, it's not a surprise that IT generally manages the deployment and maintenance of OT systems. While this ensures that IT knows all it needs about the OT system and that patches and firmware updates are properly managed, it doesn't mean OT doesn't face real threats.

In addition to the possibility of bad actors compromising OT devices as a way to breach the network and exfiltrate valuable data, the threat of cyber-kinetic attacks that physically damage mission-critical equipment is very real. For example, a cybercriminal could conceivably cause a CNC milling machine to overheat by preventing its cooling system from operating.

Overcoming the challenges

Despite the challenges – many of which are considerable – there is quite a lot that can be done to better protect IoT and OT devices.

The first step in protecting an organisation's IoT and OT devices is to discover them all. Gaining visibility is key to effective security and requires an up-to-date inventory of all these devices, which includes all relevant data about each device.

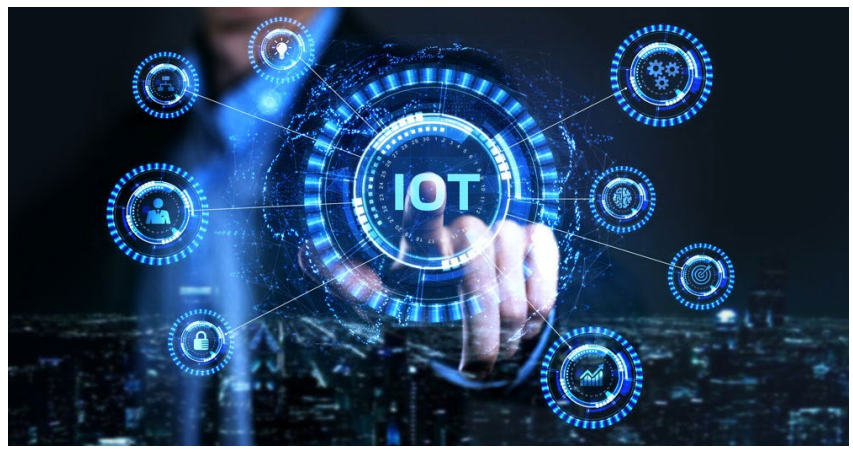
Another key element of proper cyber hygiene is installing patches. Be diligent and install patches promptly.

Monitoring is also vital. Effectively monitoring IoT and OT devices is a daunting task but is worth the effort. Fortunately, there are security services providers who can help with this.

Partnering with a security services provider is also a good option for many companies, particularly those without a security operations centre (SOC).

Companies that determine they need help should look closely at managed detection and response (MDR) providers. Their combination of 24/7 monitoring, experienced security experts and focus the early detection and response to threats make them an ideal security partner for many companies.

Though all MDR providers can monitor their customers' servers, desktops, laptops and other traditional IT assets, companies should carefully evaluate MDR providers to ensure they engage one that can also monitor IoT and OT devices. This requires MDR providers to be experts in using the latest agentless network sensors, such as Microsoft Defender for IoT. These sensors are key to an MDR provider's ability to discover customers' IoT and OT assets, ingest telemetry from these devices and to continuously monitor them without impacting their performance. ■



Is SD-WAN changing your enterprise into a mini network service provider? If yes, what do you need to know about your network?

Martin Saunders, product director, Highlight

Enterprise networking has gone through a massive change. It wasn't long ago when network traffic was 80% internal for accessing a local data centre or application, with 20% for the internet. The only option for the enterprise was to call on their service provider to deliver a tried and tested MPLS network to connect their locations, supported by a fully managed service.

Today's enterprise networks carry around 80% internet-based traffic as organisations take advantage of cloud data centres and online applications. This switch has enticed many to separate from their service provider and adopt SD-WAN technologies.

SD-WAN vendors promote the fact that having a managed wide area network using MPLS connectivity is now an outdated way of doing things. They emphasise the benefits of gaining independence from service providers and the removal of the many frustrations of working with such large suppliers. Not least, the switch to SD-WAN offers the ability to remove the heavy and expensive (yet reliable) MPLS network and replace it with numerous cheaper and less reliable broadband internet connections.

Whilst SD-WAN can certainly deliver on many promises, the enterprise must make an important choice. Do they adopt the SD-WAN technology with the support of a managed service provider who will configure, manage, and update everything? Or do they bring it all in-house, as many others are doing?

Going the in-house route is pushing the IT departments of these organisations into the role of a mini service provider, with full responsibility for delivering vital connectivity to their users. The enterprise must now manage, monitor, and continually improve the network, taking on all the wrap-around elements that a service provider delivered in the past. The role requires a new set of service skills in the IT department, with a new level of information they had not needed before.

Network management has traditionally fallen into the hands of highly skilled technical engineers who deal with intricate data and customisation. However, technical monitoring tools are not enough on their own for this new generation of enterprise mini service providers. Rather than skill-up expensive engineers, enterprises need tools that deliver information that can be easily understood and acted-up by their first-line support team, who have a more service orientated focus.

Service assurance is all about delivering a robust network service to all users. This requires a holistic view of an organisation's complete connectivity with insights that are suitable for both technical and non-technical users.

What are the most important metrics or features an enterprise needs?

1. An overview of all connectivity providers in one pane of glass is critical in the world of SD-WAN, where sourcing connectivity from multiple providers is becoming more common but managing them becomes harder. Enterprises need an efficient way to bring that information together in a combined and standardised view so that they can compare services and quickly identify issues.
2. IT managers have a responsibility to their users, so it's important they know about a critical issue in the network before users do. This means having the right information at the fingertips of first-line support staff. Service managers can then deal with most issues before passing to more expensive engineers. It also increases uptime and improves staff/customer satisfaction.
3. Alerts on network issues are essential but without being swamped with false positives. The ability to adjust the sensitivity of alerts is essential to identify when things have been down for a period and in need of urgent attention.
4. The IT manager will need to provide management with clear and simple reports on the performance of the network on a regular basis, requiring fast access to reliable information.
5. A service assurance tool that considers an organisation's business hours is key. This enables the IT manager to ensure the health and load on a network is not being pushed too hard when people are working or visiting a store.
6. The ability to separate the 'engineering' view of SD-WAN from the 'in-life' view required by service teams. Networks are constantly changing with new sites being commissioned and old sites being decommissioned. It's vital for service teams to have a sanitised view of what's 'live.' ■

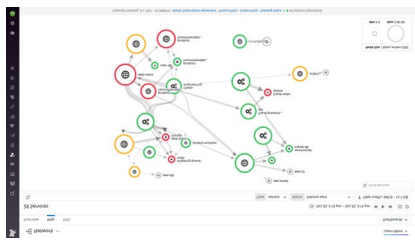
PRODUCTS

Datadog offers a software-as-a-service (SaaS) solution for network monitoring that breaks down silos between engineering teams for a holistic approach. The solution comprises a package of products to unify network data with infrastructure, application, and user experience data in a single pane of glass. Datadog provides end-to-end network monitoring across cloud, on-premises, and hybrid environments.

Network Device Monitoring (NDM) auto-discovers devices from a wide range of vendors to enable the health of individual devices to be monitored. Users can also proactively monitor device health with anomaly detection monitors for bandwidth utilization and other metrics.

Network Performance Monitoring (NPM) provides visibility into the rest of the network stack and analyzes traffic in real time as it flows across the environment. Teams can monitor communication between services, hosts, Kubernetes pods, and any other endpoint.

Datadog Synthetic Monitoring delivers additional insights from the end user perspective by utilising synthetic to determine how APIs and web pages are performing at various network levels (DNS, HTTP, ICMP, SSL, TCP). Datadog alerts the user to faulty behaviour, such as a high response time, unexpected status code, or broken feature.



PCTEL recently launched its **SeeHawk Monitor**, an automated spectrum monitoring system for P25 public safety radio and other critical communications networks. The monitor also enables automatic testing of the uplink signal to determine whether in-building coverage complies with fire code standards.

The fully scalable monitor enables continuous monitoring of spectrum across multiple radio sites; rapid detection and characterisation service impacting noise and interference; investigation of issues with spectrum analysis in real-time or event replay modes; and automatic testing of the uplink signal during in-building coverage testing.

Composed of multiple Remote Test Units (RTUs), SeeHawk monitors spectrum and radio signals at each site, while the SeeHawk Monitor Platform Manager monitors and configures all RTUs. The monitor's uplink testing feature simplifies ensuring high-quality indoor coverage that complies with National Fire Protection Agency (NFPA) and International Fire Code (IFC) standards. The SeeHawk Monitor Platform Manager remotely manages automated uplink data collection on RTUs throughout the network.

Dynatrace's software intelligence platform has been purpose-built for enterprise cloud market. The solution provides visibility and precise AI-backed answers across the entire digital ecosystem, including the digital experiences of users, application and infrastructure performance, and IT operations.

The all-in-one platform features a broad set of built-in capabilities and is fully open, enabling it to be extended with API, SDK, and plugins to ingest data and events from third-party solutions into the Davis® AI causation engine. Automation can be driven by integrating Dynatrace with ITSM and CI/CD tools.

With Dynatrace, the performance of all aspects of the environment can be monitored and analysed: real user; mobile app; server-side service; network, process and host; cloud and virtual machine; and container. Root cause analysis is also enabled.

NinjaOne offers a unified IT operations platform with an easy-to-use dashboard that reduces IT complexity and modernizes IT management. The solution delivers real-time monitoring, SNMP monitoring, and Syslog to view network health holistically.

SNMP monitoring and management capabilities include real-time polling and monitoring; hardware performance data; discovery wizard; netflow traffic data; SNMP v1, v2, v3 support.

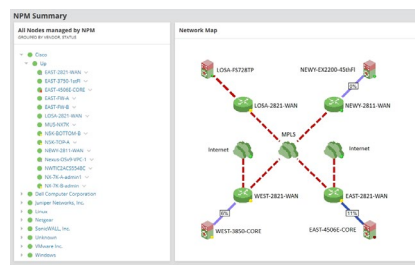
With single-pane visibility across all SNMP devices including routers, switches, firewalls, printers, IoT devices and more, combined with a remote monitoring and management (RMM) platform, NinjaOne provides a centralized and actionable dashboard for the entire IT organization.

Complete visibility into the health and performance of SNMP-enabled devices is allowed with custom OID monitoring. Any issues with SNMP devices can be discovered using hundreds of alerting conditions built into NinjaOne Network Management. NinjaOne polls SNMP devices constantly to look for abnormalities, delivering immediate results on the dashboard. Alerts can be customised by type, severity, and priority and be alerted through e-mail or SMS.

SolarWinds Network Performance Monitor (NPM) is powerful network monitoring software enabling enterprises to quickly detect, diagnose, and resolve network performance problems and outages.

Features include speed troubleshooting, which increase service levels, and reduce downtime with multivendor network monitoring. The solution measures the health of the logical network in addition to the physical network with Cisco ACI and Azure VNet gateway support. With NPM, users can simplify the management of complex network devices by monitoring the right information for each device's unique role in the network with Network Insight™ features. Critical path hop-by-hop analysis for on-premises, hybrid, and cloud services are enabled, as is cross-stack network data correlation for acceleration of problem identification with the PerfStack dashboard. Improved operational efficiency with out-of-the-box dashboards, alerts, and reports are another benefit.

Scalable up to 1 million elements per instance, SolarWinds NPM gives enterprises the ability to troubleshoot VPN issues with a clear picture of both sides of their VPNs for improved connectivity.



Please meet...

Russ Kennedy, chief product officer, Nasuni

Who was your hero when you were growing up?

I was very active growing up, playing all kinds of sports. I played baseball into college and as an adult, so I could say that I had several sports stars as heroes in my early years. My dad was also my hero as he encouraged me to be active and to compete with maximum effort - but always to respect my opponent. But my mom was actually my hero. She was a teacher and all throughout my formative years, I also wanted to be a teacher. She convinced me that I would need a good education in a field that I could build a career and achieve financial success, which is not usually found in teaching, but that I could actually be able to teach others in most any field I chose for my career – and she was correct.

What was your big career break?

I graduated with a degree in computer science and went to work as a software developer in aerospace. I changed jobs several times but realised I wasn't a great developer, although I found I really enjoyed working with people. So, I went back to school and got an MBA and worked my way into management.

As a young manager, I was given the opportunity to take over an entire software division within a larger, mostly hardware-based company, and take responsibility for a large and profitable revenue stream. I was one of the youngest executives leading a division made up of development teams all over the world.

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

Since I couldn't make it as a professional baseball player, I wanted to go into teaching. My mother convinced me to seek another profession that would be more financially rewarding, so I started in software development.

I taught my own children to be active and participate in sports and I coached them as well as other youth teams as my career progressed. I've always enjoyed working and mentoring kids. I will volunteer a lot more in youth programs once my professional career comes to an end.

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

John F. Kennedy. As a kid growing up, I was always fascinated by a US president with the same last name as mine. My first vivid memory is seeing my mother cry while watching the news that he had been shot - I was four years old. I think he was the last great leader the US has had, unfortunately. Had he continued through his full term in office and post presidency, I think the world would be a much different place right now.

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

Don't ever take anything for granted. Things happen for a reason and usually that reason is due to someone or a group's effort, ingenuity, creativity, organisational skills and teamwork. If you take things for granted and don't leverage your developed skills and the people around you, the results you achieve will not live up to your expectations.

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

I'd probably work in the adventure travel industry. I enjoy travel with lots of physical activities (hiking, biking, kayaking, etc.) and it would be energising to lead or guide a group of people on those adventures. Most people want to relax when they travel but I'm the opposite. I get bored if there's not plenty of physical activities to keep me busy and let my mind clear: I'd like to guide others that enjoy that same type of vacation activities.

The Rolling Stones or the Beatles?

Both are iconic and the Stones have certainly had longevity, but you can't dismiss the impact the Beatles had when breaking into the music scene. Because of that, I'll go with the Beatles.

What would you do with £1m?

I would invest a portion for the security of my family over the long term. Whenever I've come into unexpected sums of money, I've generally invested it for a specific goal, like college expenses for my children and I see this in the same way. I'd also give a portion to a charity so others can benefit from my good fortune. And the remainder, I'd probably use for an adventure vacation (see above).

Where would you live if money was no object?

I always tell people I live in one of the best places in the world in the front range of Colorado. There's plenty of outdoor activities and the climate is relatively but still with four distinct seasons.

Recently, I traveled to Switzerland on an adventure vacation and fell in love with the region. We were mostly in the Alps, and I found it very similar to where I live now, with a slower pace but a real passion for life. My wife has family roots in northern Italy which is also very similar, and I could see myself living there as well!

Bottom line: if money is no object, my choice would be to have a place in all three and enjoy each area. ■