SEPTEMBER 2022
networkingplus.co.uk

NETWORKING+

Preparing for an uncertain future
Some tips on business continuity
Mark Adams, Cohesity, p6

The future of education
Laying the network foundation
Kyle Davies, CDW UK, p7

Questions & answers
'I'd love to meet Barack Obama'
Jed Ayres, IGEL Technology, p16

Ofcom probes Amazon, Google and Microsoft over cloud dominance

Media regulator Ofcom is investigating Amazon, Google and Microsoft's dominance of the UK's £15bn cloud computing industry.

The watchdog will launch a study to ascertain the position of firms offering public cloud infrastructure and whether they pose any barriers to competition, it said.

Ofcom's probe will focus on so-called 'hyperscalers' like Amazon Web Services (AWS), Google Cloud and Microsoft Azure, which let businesses access computing power and data storage from remote servers, instead of hosting it on their own private infrastructure.

The review will form part of a broader digital strategy push by Ofcom, which regulates the broadcasting and telecommunications industries in the UK.

Further action could be taken by the watchdog if it finds the companies' actions are harming competition. Selina Chadha, Ofcom's director of connectivity, said the regulator had not yet reached a view on whether the cloud giants are engaged in anticompetitive behaviour. Ofcom said it will begin its investigation in the coming weeks, then will conclude its review and publish a final report including any concerns and proposed recommendations within 12 months.

"The way we live, work, play and do business has been transformed by digital services," Chadha said in a statement. "But as the number of platforms, devices and networks that serve up content continues to grow, so do the technological and economic issues confronting regulators. That's why we're kick-starting a programme of work to scrutinise these digital markets, identify any competition concerns and make sure they're working well for people and businesses who rely on them."

Cloud computing represents circa 17% of businesses' global IT spending, according to Ofcom, with Amazon, Google and Microsoft taking a combined 81% share in the cloud infrastructure services market in the UK.

Amazon leads the cloud infrastructure services market, with AWS recording $62.2bn of revenue and over $18.5bn in operating income in 2021 alone.

Microsoft's Azure is in second place, Google is the third-largest player. Other key players operating their own cloud arms, include IBM and China's Alibaba.

"Our study will formally assess how well this market is working," Ofcom said in a statement. "We will examine the strength of competition in cloud services generally and the position the three hyperscalers hold in the market. We will also consider any market features that might limit innovation and growth in this sector by making it difficult for other companies to enter the market and expand their share."

The regulator added that because the cloud sector is still evolving, it will examine how the market is working today and "how we expect it to develop in the future – aiming to identify any potential competition concerns early to prevent them becoming embedded as the market matures."

Commenting on the probe into competition cloud market, Paul Stone, senior counsel at international law firm Charles Russell Speechlys, said the move is indicative of increasing scrutiny being placed on the big tech sector by UK competitions regulators.

"The market study may act as a catalyst for a full-blown market investigation, which could have a significant impact on big tech firms," he said. "Given that Ofcom appear to be concerned about market entry, measures they could implement include limiting any exclusivity arrangements used by the 'hyperscalers' or requiring interoperability with new players."

Amazon, Google and Microsoft were not available for comment when contacted by *Networking+*. ■

IN DEPTH: Time to upgrade? pp8-10

Neos connects Viking Energy Wind Farm to SSE Renewables headquarters

Neos Networks will provide crucial communications links between the Viking Energy Wind Farm, being constructed in Mainland Shetland and the headquarters of SSE Renewables, in Perth on the Scottish mainland, more than 300 miles away.

The Viking Energy Wind Farm is one of the largest projects of its type in the UK and when fully operational will power homes and businesses across the UK. It is expected to generate £2.2m annually in community benefit revenue for the islands for its expected 25-year operational lifetime.

Neos will provide a machine-to-machine (M2M) network, which will enable the energy provider to control and monitor the performance of the 103 wind turbines remotely – and provide links back from Shetland to SSE's headquarters in Perth.

Performance data can be monitored locally and back at SSE Renewables headquarters to ensure the farm is operating at maximum efficiency, with the M2M comms across the entire site also highlighting any potential issues and enabling preventative maintenance.

"With any new facility of this size, scope and importance, deploying and provisioning first class communications links are critical to its operational performance," said Andy Ainsley, head of energy and utilities at Neos Networks.

The provision of connectivity infrastructure, in tandem, of an undersea 600-megawatt high voltage power cable is vital to delivering the project, enabling the islands to generate wind power for the rest of the United Kingdom. ■

'Ransomware attacks continue increasing', says report

Nearly a quarter of businesses have suffered a ransomware attack, with a fifth occurring in the past 12 months, according to the latest annual report from cybersecurity specialist Hornetsecurity.

The 2022 Ransomware Report, which surveyed over 2,000 IT leaders, revealed that 24% have been victims of a ransomware attack, with one in five (20%) attacks happening in the last year.

Cyberattacks are happening more frequently. Last year's ransomware survey revealed one in five (21%) companies experienced an attack; this year it rose by three percent to 24%.

"Attacks on businesses are increasing, and there is a shocking lack of awareness and preparation by IT pros," said Daniel Hofmann, chief executive officer, Hornetsecurity. "Our survey shows that many in the IT community have a false sense of security. As bad actors develop new techniques, companies like ours have to do what it takes to come out ahead and protect businesses around the world."

The survey also showed that more than one in five businesses (21%) that were attacked either paid up or lost data. ■

Revolut confirms data breach of 50,000 users

The UK's most valuable fintech startup Revolut confirmed it was hacked in September, exposing data on more than 50,000 customers around the world.

News of the breach was disclosed on Friday, September 16 to the state data protection agency of Lithuania, where the company holds a banking licence.

The hack occurred the night of September 11 and affected just 0.16% of its customers, according to an email sent by the company to users who have been impacted by the attack.

London-based Revolut is valued at £29 billion according to Forbes and has over 20 million users in 200 countries, but it most popular in Europe and the UK.

The company said that it suffered "a highly targeted cyberattack from an unauthorised third party" that may have gained access to some of the user data for a short period of time. Revolut said exposed information varies for different customers, but mostly includes user names, addresses, emails, postal addresses, telephone numbers and part of the payment card data. Rick Jones, chief executive officer and co-founder, DigitalXRAID, said news of the Revolut data breach comes just weeks before the tenth anniversary of Europe's Cybersecurity Awareness Month – this year focused on phishing attacks and highlighting why an individual should 'Think Before U Click'. He added: "Considering Revolut's breached customer data is now being used within targeted phishing and smishing attacks, it is critical that Revolut users stop and think before they click on any links and keep cybersecurity front of mind, to avoid any personal loss."

Ian Farquhar, field chief technology officer (global), Gigamon said that while they may seem simplistic hacks for such a large organisations, social engineering and phishing attacks are becoming increasingly common and successful routes for cybercriminals.

"The insider threat is not to be underestimated – our recent research actually found that 71% of UK IT and Security leaders had seen phishing emails as a route for ransomware in the last year," he continued. "While the workforce can be the first line of defence for an enterprise, they can also be susceptible to scams and accidental clicks that lead to huge disruption."

Revolut reassured customers that no funds were stolen and no card details, PINs, or passwords were accessed.

Jones added that to protect their networks, organisations should also make use of phishing simulation services consulting on best practice with expert security partners, to test employees against the current and most dangerous scams and give feedback on how well they performed.

These exercises should be run often to reinforce good cyber hygiene and ensure security is always kept front-of-mind.

The Revolut app was founded in 2015 by Russia-born Nikolay Storonsky and Ukraine-born Vlad Yatsenko. ■

Gov issues new AI security guidance

GCHQ's National Cyber Security Centre (NCSC) has released new guidance designed to help developers and others identify and fix vulnerabilities in machine learning (ML) systems.

The nation's leading security agency put together its *Principles for the security of machine learning* for any organisation looking to mitigate possible adversarial machine learning (AML).

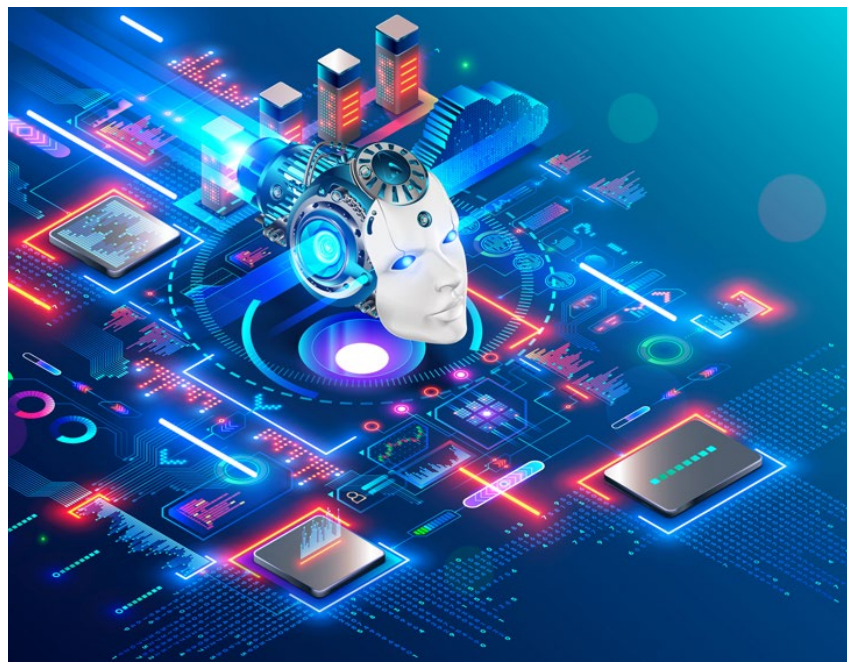
AML, which exploits the unique characteristics of ML or AI systems to achieve various goals, has become a major concern as the technology finds its way into an increasingly critical range of systems, underpinning sectors such as healthcare, finance, as well as national security.

"At its foundation, software security relies on understanding how a component or system works," said Kate S, NCSC data science research lead. "This allows a system owner to test for and assess vulnerabilities, which can then be mitigated or accepted. Unfortunately, it's hard to do this with ML. ML is used precisely because it enables a system to learn for itself how to derive information from data, with minimal supervision from a human developer. Since a model's internal logic relies on data, its behaviour can be difficult to interpret, and it's often challenging (or even impossible) to fully understand why it's doing what it's doing."

The new principles will help any entity "involved in the development, deployment or decommissioning of a system containing ML."

They aim to address several key weaknesses in ML systems, including reliance on data and reverse engineering.

"In the NCSC, we recognize the massive benefits that good data science and ML can bring to society, not least in cybersecurity itself," Kate S added. "We want to make sure those benefits are realised, safely and securely." ■



EDITORIAL:
Editor: Amy Saunders
amys@kadiumpublishing.com
Designer: Ian Curtis
Sub-editor: Gerry Moynihan
Contributors: Robert Shepherd, Abirami A, Nathan Howe, Kyle Davies, Scott Davis, Mark Garner, Mark Wharton, Chris Berry, Knud Kegel, John Hall, David Sandars, Matt Edgley, Eric Herzog, Simon Brady and Richard Clifford

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

Three UK and Freshwave to combat poor mobile 4G indoor connectivity

Three UK has partnered with Freshwave on the operator's first deployments of the Neutral Host In-Building mobile specification. Following two successful pilot tests at Workspace's offices in London, the approach has been selected by Three UK to augment its 4G indoor connectivity.

Some 80% of mobile phone calls originate from indoors, but modern building materials make it more difficult for the outdoor macro signal to penetrate inside. As a result, many buildings harbour mobile signal dead zones which can reduce business productivity and increase both employee and client frustration. Accordingly, in-building small cell systems bring network indoors with guaranteed quality of service, without placing extra pressure on the outdoor macro.

A standard for in-building radio solutions, the Joint Operator Technical Specifications (JOTS) Neutral Host In-Building, has recently been established in collaboration between all four of the UK's mobile network operators. It specifies the technical standard use of 4G small cell technologies to simplify the provision of indoor mobile coverage for businesses.

By adhering to the JOTS NHIB specification, a third party, or 'neutral host' can provide mobile services to businesses on behalf of one or more of the operators. The neutral host can enable this connectivity using their own choice of vendors and equipment.

"Indoor focus has been a major priority of ours with the acquisition of additional low frequency spectrum in 2020 and our agreement with Freshwave will further enhance indoor coverage, particularly for business customers," said Iain Milligan, chief network officer at Three UK.

"This is another step forward in making assured indoor mobile connectivity easier for businesses to access around the UK and we're pleased to have worked with Three UK on this world-leading approach," said Tom Bennett, CTO at Freshwave. "We're excited that Three UK is now also using the specification and that Freshwave is the first company to be the neutral host for multiple operators on the NHIB specification."

"I'm proud that Workspace provides premium spaces for our customers and that we have the premium mobile connectivity they want and need," said Chris Boultwood, Head of Technology at Workspace. "Freshwave have been our mobile connectivity partner for many years now and ensure that we remain up to date with the changing technologies available." ■

STL divests IDS as part of portfolio realignment

Indian data network solution specialist STL has announced its divestment of Impact Data Solutions Limited (IDS), UK, to Hexatronic Group as a part of a consolidated strategy to focus on core business segments of optical solutions and global services.

The former will sell its equity in IDS to the Gothenburg-headquartered firm for an initial consideration and an earn-out upside.

In recent years, IDS has been operating in certain niche areas of the data-centre market, primarily inside-data-centre connectivity and containment solutions. It is understood this move will help IDS achieve future success and enable the Mumbai-based company to strengthen its core business and balance sheet. Going forward, STL will continue to evaluate non-core assets and take prudent decisions to re-balance its portfolio and optimise capital allocation, the statement said.

"As we take our company towards focused growth in this decade of network creation, our efforts and capital allocation will be fully aligned towards optical and global services businesses," said Ankit Agarwal, managing director, STL. "We will continue to calibrate and realign our portfolio to enhance profitability, increase shareholder value, and drive towards our purpose of transforming billions of lives. We are proud of the value that we have co-created with IDS and wish them the best for the future." ■

Cognizant becomes Freshfields' new tech partner

Cognizant has partnered with international law firm Freshfields Bruckhaus Deringer to manage global IT operations and support its global expansion plans. Under the new multi-year agreement, Cognizant will provide a 24x7 managed service of Freshfields' IT infrastructure and applications, as well as managing its service desk. Cognizant will also help define Freshfields' technology transformation roadmap. "Many legal services firms are at an inflection point and are beginning to accelerate digital transformation and modernise their enterprises," said Manju Kygonahally, head of communications, media and technology, global growth markets, Cognizant. ■

Connexin targets Scarborough and Cottingham

Infrastructure and connectivity specialist Connexin is expanding its full fibre network to enterprises in Cottingham and Scarborough in Yorkshire, as part of its commitment to bringing broadband connectivity to enterprises in the north. The company said this is part of its plans to 'level up' the north through digital connectivity and enablement. Since the start of its rollout last year, Connexin, which was founded in Hull, has had the intention of expanding. Ashley Achmed, head of FTTP delivery said "We're on a continious mission to become the biggest Alt-net in the North to lessen the digital divide seen throughout the country." ■

Couple deleted hotel data 'for fun'

Hackers carried out a cyberattack against Holiday Inn owner Intercontinental Hotels Group (IHG) "for fun". The BBC reported how two people, describing themselves as a couple from Vietnam, say they first tried a ransomware attack, then deleted large amounts of data when they were foiled.

They accessed the hotel chain's databases thanks to an easily found and weak password, Qwerty1234. The hackers, calling themselves TeaPea, contacted the BBC on the encrypted messaging app, Telegram, providing screenshots as evidence that they had carried out the hack. UK-based IHG operates 6,000 hotels around the world, including the Holiday Inn, Crowne Plaza and Regent brands. ■

Delinea opens new UK data centre

Delinea, the privileged access management (PAM) solutions specialist, has opened a new data centre in the UK, offering enterprises "security, flexibility and performance they need to protect their digital assets". It said the new site further enhances the company's cloud infrastructure to meet the growing demand for cloud-based PAM, offering customers increased deployment options and better serving organisations with stringent data residency requirements. Delinea has existing facilities in Canada, east and west Coast US, Germany, Singapore and Australia. "The new data centre provides customers with the security, flexibility and performance they need to protect their digital assets," said Spence Young, VP EMEA at Delinea. ■

ng-voice, Casa partner for cloud-native solutions

ng-voice has partnered with Casa Systems to deliver fully cloud-native products to enterprises. The former's fully containerised, Kubernetes-based IMS core combined with Casa's 4G/5G multi-access core solution will simplify deployment and management of public and private networks reducing time-to-market and resource requirements, the companies said. "Our joint end-to-end fully containerised and cloud-native network solution can equal a smaller resource footprint, reduced cost, and greater value for our customers, unlocking true future-proof competitive advantages," said David Bachmann, chief executive officer, ng-voice. We're delighted to partner with a company that has the same mission to provide a disruptive solution to the market." ■

'Largest cloud spend in next 24 months'

The next two years could see a rapid acceleration in the pace of cloud adoption by enterprises, according to new research from datacentre network connectivity provider Colt. In the company's third annual Cloud adoption report, 500 senior IT and C-suite decision-makers from Europe and the Asia-Pacific region were asked about their off-premise migration priorities for the years ahead. Half of the respondents (50%) indicated that they plan to step up the amount they are investing in cloud over the next 24 months, with the intention of picking up the pace of their off-premise migration efforts. ■

Security experts protect construction projects

Construction firms working together on major building projects have been offered "first-of-its-kind" security advice from industry and government. The new Information Security Best Practice guide aims to help these firms keep sensitive data safe from attackers by offering tailored advice on how to securely handle the data they create, store and share in joint venture projects. The guide is a collaboration between experts from industry and the National Cyber Security Centre (NCSC), the Department for Business, Energy and Industrial Strategy (BEIS) and the Centre for the Protection of National Infrastructure (CPNI). It includes input from firms with experience in joint ventures, including major infrastructure contracts such as HS2 and Crossrail. ■

Wallix, Nozomi join forces

Wallix and Nozomi Networks have forged an alliance to deliver advanced cybersecurity solutions to OT and IoT environments. Under the terms of the deal, the companies aim to provide "end-to-end visibility" and "traceability for maximum security" in an industrial environment. "Partnering with Nozomi Networks to provide a zero-trust approach and complete visibility into the entire OT third-party journey seemed an obvious choice," said Yoann Delomier – Wallix OT team leader. "The correlation of traceability and visibility data from our two platforms offers analysis and detection power." ■

Tech Data appointed as a distributor for Pure Storage in the UK

Tech Data has teamed-up with Pure Storage to get the latter's technology in front of more UK resellers. The distributor, which views its new partner as a complementary vendor to its existing portfolio, is charged with both serving existing Pure partners and introducing additional resellers. "As the capacity needs of large and mid-sized organisations continue to rise, there are tremendous growth opportunities for partners with Pure Storage," said Jason Boxall, senior vice-president of advanced solutions for EMEA at Tech Data. ■

Word on the web...

Adopt a cyber-secure mindset

Simeon Tassev, MD & QSA at Galix Networking

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

Preparing for an uncertain future; building a solid data centre business continuity strategy

By Kate Fulkert, global business continuity and disaster recovery manager, Vertiv

As we all discovered over the last two years, and more recently, anything can happen at any time. Organisations need to be ready to pivot operations quickly and efficiently as and when needed. Business continuity has never been more important, and a company's data centre strategy is paramount in keeping operations running and businesses open.

Dealing with the threat of civil unrest

One year ago, the ongoing pandemic dominated planning exercises, with the fallout of the Covid-19 crisis continuing to rock businesses of all sizes. But today we are spending more time on civil unrest and extreme weather conditions than any other threat.

In addition to the devastating destruction and health and safety concerns for those in the country and in nearby regions, the war in Ukraine has dramatic implications globally. Further strain has been put on supply chains, severely restricting commerce in Ukraine and Russia, and limiting communications with employees, suppliers and customers in those countries.

The war is taxing the systems in place and creating an environment that attracts bad actors, including cyber criminals. It's an ongoing and increasingly volatile situation, and sadly will be for the foreseeable future. Accordingly, organisations should work to develop business continuity and disaster recovery plans for employee communication, transportation, supply chain and workflow, whilst ramping up cybersecurity training at all levels.

Protecting organisations in the move to mass remote working

Prompted by Covid, but here to stay, the widespread shift to remote or hybrid models continues to cause challenges, not least a significant increase to the threat of cyber attacks. A distributed workforce means a boost in network endpoints, and each endpoint represents a cybersecurity risk. If your business is shifting to remote or hybrid work models, you must increase attention on network security and ramp up employee training on IT and operational security.

Organisations must also consider how they will track and communicate with employees in an emergency. They should invest in platforms that can enable critical communications, even when traditional channels are down, and update crisis management training so employees know how to react independently.

A twelve-point plan for success

Here is some guidance on the components to include in successful crisis preparation:

1. **Risk assessment and the Business Impact Analysis (BIA):** The critical first steps for a comprehensive recovery strategy. Perform the BIA to determine critical business functions and a risk assessment to identify potential mitigations or controls that should be implemented.

2. **Weatherproof the data centre:** Create a severe weather checklist and train employees how to prepare for extreme weather conditions; severe weather conditions are increasing globally and will continue. Consult with a data centre service provider that can help harden the data centre and edge facilities against severe weather threats as certain critical infrastructure may require uninterruptible power supply (UPS) backup power or redundant internet service providers. On your checklist, add physical procedures to be verified, such as ensure all doors and windows are shut tight, clear downspouts and drains, and remove or secure any outdoor equipment or movable fixtures.

3. **Network redundancy:** Build network redundancy into your data centre; ensure you have redundant core and edge infrastructures along with multiple fibre vendors to reroute traffic in the event of an interruption in the network path. Conduct a network system check two times each year to detect any deficiencies and / or identify risks or gaps. Other tips for the network include building resiliency into mission critical network segments, documenting all changes and upgrades, maintaining an inventory of network devices and where they are located, increase UPS capacity when expanding or adding to your network, and conducting a "network" disaster recovery test annually.

4. **Backup data:** The process changes as employees shift offsite. Automatic backups on-site may need to be initiated manually, and the mechanics - including backing up data to the cloud - should be hardened against cyber threats.

5. **Preparation for communication breakdowns:** A remote workforce introduces challenges related to emergency communications. Develop lists with all available means of communication for all employees and reach out early with instructions in the event of communication interruptions. It is essential to validate all forms of communication and exercise your communication strategy quarterly.

6. **Emergency staffing:** The preference for many companies today is to shift work virtually, but staff on site may still be required, and needed immediately; have an emergency staffing plan in place.

7. **Contact vendors:** As supply chains continue to lag, businesses should consider adding vendors and suppliers to their mass notification systems to ensure critical communications are maintained.

8. **Move away from a single vendor approach:** Critical business functions should have more than one vendor in place in the event that vendor has a supply chain issue. Don't single source vendors, instead have two to three vendors in your recovery plan to provide products and services.

9. **Build team redundancy and train on emergency response:** At Vertiv we talk a lot about trusting our teams and that's still important, but it's also critical today to build redundancy across teams to ensure all team members have a backup. Along with team redundancy, train team members to be prepared for various types of crisis events at work, home or out in the field. Conduct training so they can react to a crisis independently – include relevant resources in the community and information on who to contact. Employees should take advantage of weather and emergency phone apps too.

10. **Inform and work with first responders:** Many insurance providers are asking for floorplans to be shared with first responders. It's a good idea, and one any organisation should insist upon even if the insurance provider isn't. Taking photographs of the data centre prior to a disaster event is good practice; before and after pictures make it easier to work with insurance providers.

11. **Consider the opportunists:** Chaos provides cover for cyber criminals. Training employees on cybersecurity best practices is more critical than ever with the shift to remote work.

12. **Test your plans:** Vertiv has increased testing of plans twofold this year and is expanding on the types of tests we perform, for example, we are adding more shelter in place and speed drills to crisis response. Testing does not need to be complicated but is the best means to get recovery plans communicated.

So, whilst the threats and risks to businesses across the world are changing, the need to prepare adequately with robust Business Continuity strategies is not. Crucially, processes, policies and plans must begin with protecting the critical infrastructure which keeps businesses up and running – not least in the data centre. ■

The importance of disaster recovery to the security solution

Mark Adams, regional sales director, northern Europe at Cohesity

The blast radius of ransomware has evolved and expanded with dirty new tactics each year, and everything points towards the problem getting worse before it gets better. On average, victims of ransomware only recover around 65% of stolen data after paying the ransom, mostly due to the technical faults in the ransomware itself. The only way to reduce the threat is by minimising the impact of ransomware attacks themselves; once it's not an easy money-maker, the attacks will become less frequent. Ransomware is a disaster; treat it like one and prepare for it. That means making sure the business can survive an attack without paying a ransom, recover quickly from it, and keep your services or products available.

To do this, first, focus on increasing the frequency of good quality backups of your data that can be relied on for recovery. Second, ensure that the backup data is safe from attack and can't be changed (immutable copies of data is the technical term to look for). Third, make sure you can access the backup quickly and easily, for example, by using a secure cloud-based data isolation service. Making your business' data recovery unassailable is the key now.

Ensuring you have a disaster recovery plan in place

A disaster recovery plan (DRP) is a documented, structured approach that describes how an organisation can quickly resume work after an unplanned incident. A DRP is an essential part of a business continuity plan (BCP).

Today threats have evolved to be much more nefarious with the rise of ransomware. According to research by Cybersecurity Ventures, every 11 seconds a business falls victim to ransomware. For many customers, this is now the most serious concern. However, many organisations are also concerned about natural disasters like floods, hurricanes, large-scale power outages, or even human error – all these factors can impact the availability of data and services.

Regardless of the outage, the objective for recovery remains consistent: recover as much data as possible, as quickly as possible, to enable the organisation to continue operating.

With cyberattacks, organisations must consider a key challenge: making sure that the data you're recovering doesn't contain the same trojans or viruses that enabled the attack in the first place. This is why the industry has always recommended a 3-2-1 backup strategy - three copies of data, on two different media, with one of them in an off-site environment.

Not all data is equal. The first thing organisations need to understand is - what data needs to be protected and have proper alignment across the functions. Organisations also need a clear understanding of their recovery SLAs, along with the dependencies. And finally, they should test often to know if they can consistently meet their recovery SLAs.

The absence of any of these can impact the recovery. Traditionally, organisations have relied on multiple point products for their backup and disaster recovery. These solutions are often incompatible, create data sprawl, and make it hard to test application interdependencies or recoverability.

A single platform that consolidates multiple use cases (Backup, CDP, and DR), allows organisations to run multiple services together to clearly identify application dependencies and ongoing testing. With ransomware being one of the primary threat vectors, it's also critical for a robust data recovery plan to also include backup. Modern backup solutions also provide immutability which are designed so that backup data cannot be deleted or altered and this is critical in protecting an organisation's data against ransomware.

Downtime can have dramatic effects on businesses and can take the same out of business. Organisations need to balance the risk and the investments. Whether it's about investing in new areas or choosing to cut spending in others, businesses must assess their balance of priorities given the potential for success or failure – and that's an issue for technology, security and disaster recovery.

Some of the most challenging situations arise when attacks have the potential to put lives at risk. There have been well publicised examples of hospitals being attacked by ransomware, where a lack of data availability could directly impact patient care.

For example, a US-based hospital suffered a critical ransomware attack, potentially crippling its infrastructure. With Cohesity, the hospital was able to recover machines and file shares, verify they're clean, and quickly bring the applications back online, saving hundreds of hours of work without having to pay the ransom. Even more important, the hospital was able to continue to focus on providing high-quality patient care.

While these types of cyber attacks have the potential to put lives at risk, they also show why it's so important to have a next-gen data management solution in place that can strengthen security, bring applications back online quickly, and help organisations rapidly recover. ■

Laying the network foundation for the future of education

Kyle Davies, head of solutions at CDW UK

The opportunity to build a network from the ground up, tailor made to accommodate a state-of-the-art campus fitted with modern technology, does not come along very often. That was the case, however, when CDW was awarded preferred supplier status from the University of Birmingham to conceptualise the modern-day campus network for their brand-new tech-led campus in Dubai. The contract presented a unique opportunity to assess the need, map out a tailor-made solution, configure and test it in our state-of-the-art Distribution Centre in Rugby, UK, ship it and from there allow our team in Dubai to seamlessly plug and play.

As a first step we sat down with people across the organisation to understand both the functional and non-functional requirements of the network, as well as wider programme of work. We were rigorous in mapping stakeholders – from the research team, estates, facilities team, IT team and even the students themselves to understand exactly what they wanted and how they intended to consume services on the network. This formed the basis of our recommendations to deliver a robust and modular platform for innovation and growth in the years to come.

Once we had the insights and requirements, we mapped them to an actual network level design and then configured the entire network in our warehouse in Rugby, UK. At the time, the University campus was still being built and by configuring it in advance were able to meet the tight project timeline as well as saving the customer time and money through managing procurement cycles. Working closely with other partners, we knew exactly what the network had to deliver to connect a smart building to a network securely. That's where technologies like Wifi-6 become an absolute game changer.

Wi-Fi 6 is presenting an opportunity for organisations across the board to fundamentally change the way they provide access to services. This is largely because of increased demand on media rich content, as well as the increasing number of high-end devices present. If you consider a campus, or even an office, 10-years-ago any given person may have had a standard issue laptop and a phone. Part of the exploration phase of our project included looking at how many unique devices were being used per student at the University's UK campus today – that number was circa 3.5.

If you match this up with people's attitudes – Wi-Fi today is considered a basic right, no longer a nice to have but something that frustrates people if it is not there, or worse, does not work. Wi-Fi 6 not only allows us to provide high density, high performance, and high throughput connectivity; compared to Wi-Fi 5 it also increased the amount of capability on wireless access points and networks.

Wi-Fi 6 uses orthogonal frequency division multiple access (OFDMA) to support high density deployments, allowing multiple users to access networks at the same time with no lapse or down time. Simply put, it means we're getting more out of every transmission so that every time we go out to the network we are capable of sending more data. This matters for any organisation that is getting bigger, or in this case a learning environment that is considering expanding into eSports, gaming, high end research or distance learning. All of this relies on the switches that enable the Wi-Fi network to function.

Our first consideration for security is that we ultimately have to enable choice. Unlike many traditional enterprise scenarios where approved laptops and devices are distributed to employees, we needed to consider the wide variety of devices that may be brought onto campus. Our job is to secure these devices to allow the students to do what they need to do without compromising the network.

Having a centralised management platform that dynamically updates based on the user, the type of device and what they are trying to do makes it infinitely easier to manage security. This is where the beauty of intent-based networking comes to play! With intent-based networking across your campus and datacentre networks you can enable micro segmentation to put barriers between locations on the network that people are allowed access to that is based on their intent and posture.

It all comes down to software-defined networking, an overlay onto Wi-Fi 6, to keep user device and application traffic separate and provide end to end segmentation while delivering a consistent experience because the same policy is applied across the wired and wireless network. Software-defined networking also enables insights into all the traffic on the network so you can see what information is going through and make actionable insights to allow or prevent that traffic based on its intent.

Between the faster speeds, better traffic prioritisation, and added security, Wi-Fi 6 is a significant step forward in wireless network technology. It will be extraordinary to watch the impact that transforming connectivity standards will have across industries, and even the rest of society, with the University of Birmingham Dubai being just one example of how it will better the experience for its students and staff. ■

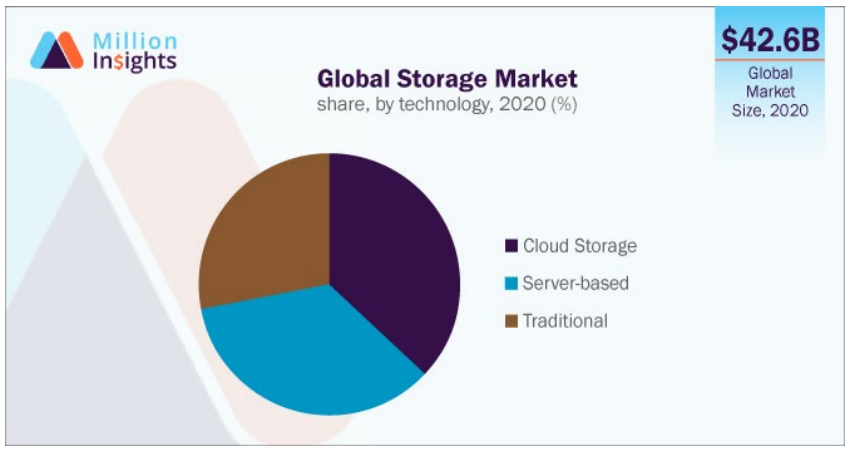
Do you need an upgrade?

With worldwide data generation increasing exponentially, enterprises are facing the pressing need to find and deploy solutions for data storage that are secure, reliable and scalable. Amy Saunders delves into the world of storage and explores several of the enterprise storage solutions available

Data is produced day in, day out, from billions of sources across the world. While the volume of data generated has been growing exponentially throughout the digital era, with more people operating more devices, and devices operating themselves, data volumes have begun to exceed even the wildest expectations off the back of the COVID-19 pandemic. With a colossal shift in workplace practises to limit physical contact and stop the spread of the virus, remote working has helped fuel a boom in demand for storage solutions, particularly highly secure cloud native products.

Why do we store so much data? One of the largest producers and users of data in the UK is the NHS, which holds the medical records for 65 million people. Those records must be updated and reviewed frequently for the patient's full lifetime in order to provide the best possible healthcare, thus the data must be securely stored and easily accessed, nationwide. Moreover, with an aging population that by definition generates more medical data, the amount of data is only going to increase, and data storage pressure will grow.

Another huge data generator is the Internet of Things (IoT). Billions of connected devices are already in play around the world, monitoring everything from pressure at an offshore oil rig to rainfall levels at a particular agricultural field. This data can be stored, analysed, and used to provide meaningful and



actionable intelligence, for example, for how often a valve is likely to need to be replaced at said oil rig, or which crop will grow best in the natural rainfall conditions at said field.

Much of the data being produced today can be monetised, either by internal use to improve processes, realising new innovation opportunities, or by sale to third parties. It would be breathtakingly wasteful then to leave that data unutilised, making storage and processing absolutely necessary.

TMI (too much information)

Data is being produced at an unprecedented rate. According to Statista, global data production hit 64.2Zb in 2020, and is expected to almost treble to 180Zb by 2025. This projection has been upgraded since the pandemic, when growth exceeded expectations due to uptake of remote and hybrid working and heavier use of home entertainment options.

Despite this production deluge, just 2% of all data created in 2020 was retained into 2021. However, even if only a tiny proportion of data is saved, global storage demands could prove immense in the years to come. Statista reported that in 2020, the installed base of storage capacity was 6.7Zb, which is expected to expand at a compound annual growth rate (CAGR) of 19.2% over 2020-2025.

Looking at revenues, Million Insights reported earlier this year that the global storage market size was valued at US$42.57 billion back in 2020 and is expected to expand at a CAGR of 5.4% over 2021-2028. Growth is being driven by improvements in storage systems which are redefining the consumption and deployment of storage solutions; the emergence of private and public cloud infrastructure; rising adoption of mobile devices by both private users and enterprise - the latter of which is finding that mobile devices deliver cost-efficiency, increased performance, energy savings and enhanced reliability; and, of course, the continually growing data volumes.

The large enterprises segment dominates the market, with a revenue share of more than 75% in 2020. However, it is the SMEs that are expected to expand at the highest CAGR from 2021-2028, with 7% growth expected. This is being driven in part by tax exemptions and government support.

The cloud segment dominated the market in 2020 with a share of more than 35%, and it is this same segment which is expected to achieve the highest CAGR for 2021-2028. Cloud storage is remarkably low cost, easy access, and is being rapidly adopted by enterprises across the world. Not only does cloud storage save the cost of maintaining an on-site data centre, but it also enables faster data retrieval irrespective of the data centre location. On the other hand, the traditional storage segment, which includes external storage devices, is expected to grow at a CAGR of 4.5% over 2021-2028.

While North America held the largest storage revenue share in 2020 at 35%, Europe comes in at a close second owing to the rising penetration of mobile devices, with the UK, Germany and France all playing a major part in said growth. The APAC region is expected to see the highest CAGR, at 7%, during 2021-2028, with countries such as China and India helping boost demand. Enterprises are investing heavily in these areas, which have large customer bases and a high rate of digital technology adoption.

So, what does that mean for enterprises? We're already seeing small, medium and large enterprises upgrading their storage systems to more user-friendly, scalable and secure solutions to meet growing business needs. We can expect to see this pattern continue in the years to come, with a heavy focus on compression and deduplication of data in order to cut both OPEX and CAPEX. The bottom line is that enterprises need smart solutions that can grow with them in order to face the data deluge.

What are some of the options?

When it comes to storage solutions, there are of course many industry stalwarts to choose from, all with their own unique offerings. Here, we look at some of the solutions for enterprise storage. Most are aimed at larger enterprises, financial institutions, healthcare, education, government, utilities, telecommunications, etc., but we've also included one option for the SME.

Amazon S3 –Fully scalable object, block and file storage

Amazon Web Services (AWS) offers several cloud storage solutions, and users can pick from object, block and file storage services.

The company's top product, Amazon Simple Storage Service (Amazon S3), offers object storage with full scalability, and promises to store and protect any amount of data for a wide range of use cases, including data lakes, cloud-native applications, websites, backups, archive, machine learning and analytics. Designed for 99.999999999% (11x9s) durability, Amazon S3 leads the storage market in terms of revenue and data quantity.

Users can store data in Amazon S3 by working with an organisation from the AWS Partner Network (APN), which includes a variety of partners offering solutions for archive, primary storage, disaster recovery, backup and restore, and migration. To keep data secure, Amazon S3 allows users to block public access to all data with S3 Block Public access. Amazon S3 maintains compliance programmes such as PCI-DSS, HIPAA/HITECH, FISMA, and EU Data Protection Directive to help the user meet regulatory requirements.

AWS also offers Amazon Elastic Block Store (Amazon EBS), a block storage service offering an easy-to-use, scalable solution for Amazon Elastic Compute Cloud (Amazon EC2), delivering 99.999% durability.

There's also AWS Backup, a fully managed, easy-to-use backup service that centralises and automates data backup across AWS in the cloud and on premises. The cost-effective solution helps support regulatory compliance and business policies for data protection.

Cloudian Hyperstore – Cloud native object storage with robust security

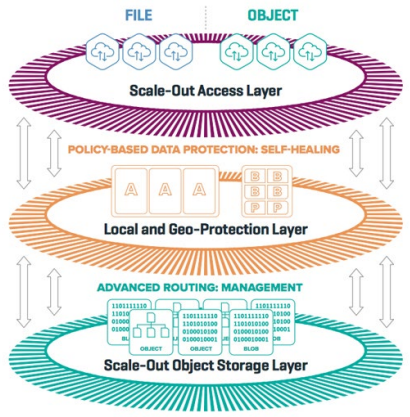
Cloudian offers simple, modularly scalable, cloud native object storage. S3 compatible Hyperstore enables organisations to store data across sites, on containers, servers, virtual machines or the cloud, within a single, unified platform. With HyperIQ, a single screen overview of the entire data environment is provided, making it easy to monitor user behaviour and spot performance or compliance problems.

Hyperstore seamlessly integrates with AWS, Microsoft Azure and Google Cloud, and uses the provider's tools to copy and move data, a useful feature for archival storage, content distribution and disaster recovery.

Key features include its robust security – Hyperstore complies with US DoD SEC Rule 17a-4(f), FINRA Rule 4511, and CFTC Rule 1.31(c)-(d) security requirements – and data immutability for ransomware protection and compliance. By utilising S3 Object Lock, cybercriminals can be prevented from encrypting data, enabling the fast recovery of unencrypted backup copy. Hyperstore allows advanced metadata tagging for accelerated data searches and easier integration with AI and machine learning analytics applications. Data is stored locally to meet governance regulations and accessed from Cloudian's all-flash or HDD-based storage with low latency. Cloudian offers appliances with pre-integrated Hyperstore software in 1U or 4U form factors, in all-flash and HDD configurations, ranging from 100TB to more than 1PB.

DataCore Swarm – Software-defined highly scalable object storage

DataCore's SWARM is an intriguing software-defined object storage solution for on premise, and private, public or hybrid cloud environments. Swarm delivers a highly scalable solution for accessing, storing and distributing data with continuous protection, boasting 25 times less downtime than traditional RAID storage, 95% storage utilisation and five times faster throughput for S3 read and write operations.



Scality RING Architecture

Swarm simplifies the management, storage and protection of data while enabling S3/HTTP access to any device, application or end user. Custom metadata with ad hoc search and query, and policy-based replication for synchronous, asynchronous and stretch cluster uses are included. It utilises a web-based UI and API and automates storage and infrastructure management, providing simplified data management that can be overseen via the unified web console, where content usage quotas and performance trends can be monitored.

Data is secured through encryption in transit and at rest, and storage access and activity can be tracked with audit trails. Data immutability is assured with WORM integration, S3 object locking and Legal Hold, while content integrity is established using Integrity Seals.

Capacity can be added, and hardware refreshed by pooling any mix of HDDs, SSDs and x86 servers, with Swarm's self-managing and self-healing architecture. Data can be searched for quickly, metadata customised, and files accessed across a single namespace via S3/HTTP, NFS and SMB. Cold data can be backed up to Wasabi, S3 Glacier and object cloud and tape storage solutions.

Dell Unity XT – Converged infrastructure for block and file storage

Dell EMC offers the Dell Unity XT family to deliver hybrid cloud and big data solutions utilising data centre infrastructure to combine storage, servers, and cybersecurity as converged infrastructure.

Dell Unity XT is a full block and file unified environment contained in a single 2U enclosure, using the same pool to host LUNs, NAS servers, file systems, virtual columns and consistency groups. It uses both storage processors to serve I/O and run data operations efficiently in an active/active manner to optimise performance, cost and density in the user data centre. The solution is managed via a simple interface called Unisphere which uses browser native HTML5.

Dell states that the Dell Unity XT family is extremely customisable. The purpose-built system can be configured as all-flash with only SSDs, or as a hybrid system with both SSD and spinning media. Dell Unity XT utilises inline data reduction to enable storage administrators to achieve more with less; Dell Unity Data Reduction works to reduce the amount of physical storage needed, providing

space savings through data deduplication and compression.

Unified Snapshots provide point-in-time copies of block and file data that can be used for backup and restoration, while asynchronous replication offers an IP-based replication strategy within a system or between systems.

Scality RING – Software-defined 'unbreakable' file and object storage

Scality's RING is a software-defined solution deployed in the user data centre, where it delivers resilient, petabyte-scale storage for archive, backup, web, video, analytics and custom applications. Deploying on any standard x64 servers, RING can scale linearly over thousands of servers, multiple sites, and an unlimited number of objects. Connectors can be co-located with customer application servers, on storage servers or on virtual machines.

Data becomes 'unbreakable' through replication, immutable object locking, erasure coding and a multi-geo distribution – which protects against data centre outages - in order to achieve 99.9999999999999% (14x9s) of durability and 100% availability. RING comes with air-gapped, tamper-proof backup data that stays immune to ransomware, offering a swift recovery from cyber-attacks.

RING supports native file, object and AWS S3 and IAM APIs interfaces, providing extremely high performance at up to 90% lower total cost of ownership than legacy storage solutions. Data-rich custom and packaged applications can both aggregate multiple workloads into a single storage environment, eliminating storage silos, and expanding utilisation with cloud-like economies of scale. RING supports all-flash storage servers too.

With hybrid cloud support, Scality's RING offers metadata-driven, policy-based data orchestration for data mobility across public and private clouds. Global metadata namespace, visibility and search is enabled across RING and public clouds, with support granted for both user and system-defined metadata. Supported storage and clouds include Amazon S3, Azure Blob Storage, Google Cloud Storage and Scality RING.

HPE SimpliVity – Hyperconverged architecture for SMEs

A unique inclusion in our review due to its recommended use cases - smaller enterprise situations, for example, retail, ROBO, small office and VDI, where applications are typically less latency sensitive - HPE SimpliVity from Hewlett Packard Enterprise (HPE) delivers hyperconverged storage by combining the entire IT stack in each node, thus consolidating up to 10 devices and applications in a building block for virtualised workloads. A hyperconverged Ai-driven architecture, HPE SimpliVity delivers self-optimising, self-managing and self-healing infrastructure.

HPE SimpliVity offers a 69% savings cost and requires no specialists to operate. It enhances its rapid backup and recovery capabilities with a centralised HPE StoreOnce long-term backup appliance and seamless cloud backup via HPE Cloud Volumes Backup.

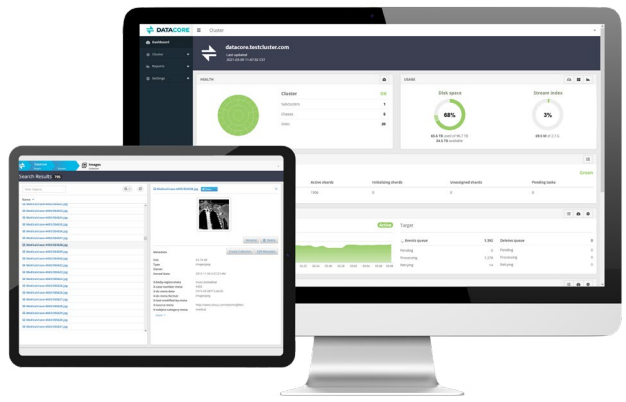
All data is stored on a least two local hyperconverged nodes for disaster recovery protection and backup, while always-on deduplication and compression reduces capacity utilisation up to tenfold. Up to 16 nodes/cluster and 96 nodes/federation makes HPE SimpliVity ultra-flexible, and it's also possible to mix clusters within the same federation. Global VM-centric management and mobility, and AI with HPE InfoSight deliver easy-to-use, intelligent management.

Two iterations exist: HPE SimpliVity 325; and HPE SimpliVity 380 - both of which can be integrated with HPE Composable Fabric, an intelligent networking fabric – and which offer varying capabilities at different price points. HPE SimpliVity 380 enables storage-intensive workloads, multiple all-flash configurations (XS, S, M, L and XL), backup and archival node with hybrid flash storage, as well as hardware-accelerated or software-optimised for always-on deduplication and compression.

Something for everyone

As we've outlined, data generation is expanding exponentially, with no sign of slowing down in the foreseeable future. As the sources of those data become increasingly diverse, having the tools in place to store, process and ultimately use that data are vital.

Each enterprise will have their own needs and demands when it comes to shaping their storage environment, but with so many storage products available on the market today, a solution can be found for every use case. Whatever form that solution takes; scalability is of the essence. Ignoring the need for ever increasing data storage could find an enterprise in a sticky situation when its systems shout "storage full!" ■



Maintaining law and order with voice and data

Scotland's COPFS upgrades legacy storage systems

Serving a nation

Scotland's Crown Office and Procurator Fiscal Service (COPFS) is the nation's prosecution service. It plays a crucial role in the justice system, working with the police and other departments to keep Scotland safe from crime, disorder, misconduct, and danger. The service investigates and prosecutes crime, establishes the cause of unexplained deaths, and investigates allegations of criminal police misconduct.

Since 2016, the COPFS has processed more than 900,000 cases. With terabytes of vital case data including documents, images, and CCTV footage, all of which must be processed, managed, stored, and accessed, the COPFS' legacy disk storage had reached its limit.

"Our data consumption was growing rapidly, and a long-term solution had to be found to avoid an operational issue we couldn't manage," says Adam Biggs, head of IT services at COPFS. "We had to take decisive action."

Moving beyond a legacy

One of the COPFS' biggest challenges was that of legacy infrastructure, which by 2021, had reached its limit. Data requirements were spiralling, and services faced disruption or being shut down entirely. Moreover, the existing approach was compromising wider environmental initiatives.

Thus, the COPFS searched for a solution that would allow it to move to the future, beyond its power-intensive legacy storage, and which would also enable the consolidation of production workloads, virtual desktops, virtual servers, Oracle databases into a stable, scalable and agile infrastructure.

The service found that Pure Storage offered a route to expand, modernise, and futureproof the COPFS' data infrastructure.

"Pure's usability, interface, and support were such a breath of fresh air from our complex legacy infrastructure. It truly empowers us to monitor, upgrade, and manage our environment in the effortless way we wanted," said Biggs.

The COPFS alleviated the immediate strain by moving its virtual servers and desktops to Pure FlashArray//X. Next, in phase two, all Oracle case management databases were also moved to Pure. The COPFS used its Evergreen// Forever subscription to upgrade to a higher model of FlashArray//X via a controller swap, without disruption and without rebuying storage. The COPFS saw a 15% improvement in core applications with Pure.

Moreover, Pure's 3:1 data reduction guarantee helped the COPFS to downsize its data centre size by 18 square feet, significantly reducing its power consumption and environmental impact. Even when the COPFS expanded capacity by a factor of five, it remained within the Pure footprint.

The icing on the cake

According to Biggs, Evergreen has been the 'icing on the cake' for the COPFS.

"Evergreen gives us OPEX predictability and the agility to upgrade and scale seamlessly, without penalty or disruption - it's incredible. We have the peace of mind that we're always going to be up to date and our costs won't spiral," said Biggs.

Pure also adds value in broader areas of the COPFS' business, such as cybersecurity, a growing challenge in many of today's businesses.

"Like most organizations, cybersecurity is a huge priority for us," said Biggs. "Pure's SafeMode™ immutable snapshots give us valuable protection and supports our cyber readiness. In a worst-case scenario, we could restore everything in our virtual server environment in a couple of clicks."

Today, some 98% of COPFS' on-premise environments run on Pure.

"The biggest compliment I can pay is that the business hasn't noticed a change. Everything works perfectly and does what it needs to do," said Biggs. "However, the impact on my team is like night and day. I no longer worry about storage because there's no reason to. Pure's technology is flawless and the ongoing service, advice, and engagement creates a partnership that's worth its weight in gold." ■

DPP Law responds to evolving telephony environment

David Phillips & Partners (DPP) Law Ltd. is home to 60 solicitor advocates, paralegals and support staff, spread across eight offices throughout England. The firm specialises in providing legal services for criminal defence, personal injury, actions against the police, and family law.

A voice service with a difference

DPP Law have been using Spitfire's PBX phone system since 2016 when the firm relocated. As part of the move, the company's telecoms provision was also re-evaluated.

"We had been using a PBX phone system located at our old head office, but we took the opportunity to see what was available on the market and evaluated several prospective suppliers," said Roger Posener, financial controller. "The 3CX system supplied by Spitfire seemed the logical choice based on our research."

3CX is an IP telephony solution available on both Windows and Linux systems. Spitfire is a 3CX Titanium Partner and supplied the 3CX system hosted in the cloud.

"With the 3CX system we just have a router at each of our offices and IP handsets. Because Spitfire hosts the service there's no need for servers or other hardware on our premises," said Posener.

Evolving workplace demands

Of course, back in 2020, the majority of DPP Law's employees were faced with the challenge of shifting to working from home in the midst of the COVID-19 pandemic. However, DPP Law was well prepared for this eventuality.

"We actually pre-empted this shift when we put new systems in place to ensure people could work from home or anywhere, they wanted," said Posener. "We didn't have any issues once lockdowns were in force as we were already offering remote working to our employees - which Spitfire enabled us to do."

Throughout the pandemic, DPP Law's employees still had to meet clients, attend court, visit police stations. The provision of reliable connectivity at all times was therefore critical. With Spitfire's solution, staff were able to access 3CX via their smartphones, keeping in touch

whenever and wherever was required.

"We had no issues whatsoever. Once the lockdowns came, this transition had already taken place, so the shift was seamless. The only difference was that more people were using 3CX from home," said Posener.

Indeed, Posener claimed that the greatest benefit of 3CX, particularly during the pandemic, was the softphone app for mobile devices.

"A lot of our staff are out of office at court or meeting clients and the app gives them full access to the 3CX service, exactly as if they were in the office, even if working abroad. This has become even more important in 2020," said Posener.

Additional connectivity benefits

Another benefit of 3CX is the conference calling capabilities. Previously, DPP Law had subscribed to a third-party conference call service, but with 3CX, a conference call can be set up quickly and easily just by adding additional callers.

Interestingly, the 3CX system uses SIP trunks for Voice over IP (VoIP) telephony instead of conventional ISDN phone lines. Designed as an ISDN replacement, Spitfire's SIP trunks offer business quality secure telephony at typically up to 50% less than the monthly rental cost of an equivalent ISDN service. Indeed, Spitfire offers a complete end-to-end SIP service via its own IP and TDM infrastructure, without using the public internet. Consequently, Spitfire offers quality of service uptime guarantees on latency, jitter, and packet loss, both upstream and downstream.

"We used Spitfire for all our data connectivity, so we had complete confidence in their ability to support our voice telephony," said Posener.

Spitfire has provided dedicated private 100Mb circuits at several of the DPP offices, which are used for voice and data. At these locations, the 3CX service is delivered over Spitfire's own Voice Approved broadband or Ethernet circuits guaranteeing the end-to-end call QoS with guarantees on Latency, Jitter and Packet Loss both upstream and downstream.

"We have never had a major outage of the service. It just does the job for everyone across the firm, no matter where they are located," said Posener. "Simply put, it has done exactly what it is supposed to."

Spitfire's SLAs emphasize fast fault response, as well as sophisticated on-line fault tracking, backed with a 'Keep Customer-Informed' policy. This ensures regular updates from a support technician who manages issues to completion. In a recent survey, 90% of respondents said an issue was resolved on first call.

The account management functionality has also been praised by DPP Law, which is provided with a dedicated account manager to discuss any changes or new services required. All in all, Spitfire has fulfilled the brief and satisfied its customer.

"We are very happy with the 3CX service hosted by Spitfire. All our offices are linked using it and our staff are pleased with the range of features, especially the mobile softphone app. It's exactly what we needed," concluded Posener. ■

How to make the most of your TETRA applications

Peter Hudson, chief technology officer, Sepura explains what TETRA has to offer

TETRA remains the de-facto choice for mission critical communications and although traditionally there has been a reliance on voice communications, users are finding it increasingly necessary to have access to mission critical data. This is vital for both improving staff safety and improving operational efficiency.

Although TETRA is often viewed as a voice communication technology, it also contains a rich and efficient mission critical data capability that is increasingly being leveraged by end users to maximise their investment in the technology. This is also helping to future proof their operations.

Users are deploying a range of applications over TETRA, designed specifically around their needs. These enable essential functions on the radios to be automated, reducing the administrative requirement on field users or control room staff, allowing them to concentrate on their primary tasks.

To enhance the use of TETRA's mission critical data capability and enable users to tailor its use to their specific needs, Sepura's radios provide an applications environment, AppSPACE. This allows user specific applications to be run on the radios and seamlessly connect teams, devices and systems with operational data, carried over their TETRA network.

Streamlining workflow and delivery of critical situational awareness information to the right people at the right time, adds operation value, predictability and effectiveness whilst reducing the dependency on voice calls.

Examples of mission critical applications include:

- AutoMate – enabling automation through geofences or automated triggers, for example changing talkgroup or sharing mission alerts with users and teams in critical locations
- SmartView – combining indoor and outdoor location, providing control room staff with accurate and timely knowledge of staff location
- RadioAudit – providing the tools to efficiently automate radio fleet audits in a fraction of the time a manual audit takes, providing an instant and traceable snapshot of the current fleet status

Applications are an example of how suppliers and user organisations are working together to enhance the use of mission critical TETRA networks using fast and efficient data capabilities to ensure user organisations can continue to enhance their capabilities and effectiveness now and into the future. ■

Preparing for the convergence between edge, IoT and networking tech

Alan Hayward, Sales & Marketing Manager, SEH Technology UK Ltd

As the industry continues to slowly recover from the COVID-19 pandemic, Forrester Research outlines the predictions that tech leaders can anticipate regarding the shifts in edge computing, IoT and networking technologies.

What can the market expect from the convergence between edge, IoT and networking tech? As the industry continues to slowly recover from the COVID-19 pandemic, Forrester Research outlines the predictions that tech leaders can anticipate regarding the shifts in edge computing, IoT and networking technologies. Altogether, it's difficult to imagine that any business wouldn't be affected by these predictions, they need to look to revolutionise connectivity in a sustainable and streamlined manner.

Looking specifically at the networking technology sector, the focus will be rising to the challenge of 5G, increase in smart infrastructure investments and the mission to reduce carbon emissions.

The evolution of 5G

IoT devices are on a staggering growth trajectory, revolutionising homes and places of work. Its potential, however, has been staggered due to a network data bottleneck - but 5G is set to be the most promising solution. Up to 100 times faster than its predecessor 4G, the new era of cellular internet will create never-seen-before opportunities, advancing everyday life. As IoT devices and their applications grow more complex, they continue to send an increasing amount of data to the Cloud. To date, the industry utilised edge computing, pushing data processing and AI capabilities from central Cloud servers to other parts of the network. This approach is now reaching its limit, meaning it's now time for 5G to take the lead.

"As IoT devices and their applications grow more complex, they continue to send an increasing amount of data to the Cloud"

In simple terms, 5G networks widen the pathway that carries data to the Cloud, which ensures the increased volume of data can be transferred at a faster speed. This results in low latency of 5G networks and can also solve the connectivity issue in rural areas. In fact, Forrester predicts that 85% of satellite internet users will be in rural locations. Looking ahead, full-scale 5G network adoption for IoT devices will require businesses to make significant infrastructure investments, which may not be feasible for all. It's important to remember that as with edge computing, 5G is essential for the next generation of IoT connectivity. Despite delays in the introduction of 5G, it is set to help the industry build a harmonious network of devices, homes and businesses in the future.

Investing in smart infrastructures

Forrester also predicts a boom in smart infrastructure for 2022, with investment expected to increase by 40%, driven by investment from China, Europe and the USA. Whilst much of that spending will go towards alleviating pandemic recovery, the investment will also be directed to internet connectivity. Early technology adopters of IoT, edge computing and 5G are already beginning to demonstrate that these technologies can empower smarter infrastructures. This highlights the opportunities that businesses can gain from leveraging data insights to modify operations and drive new projects.

As we move into the next phase of COVID-19 recovery, more and more companies and governments are investing in building a smart infrastructure as a way to make their institutions more adaptive, resilient and creative. They can also use this to launch new projects that span across emerging use cases that leverage an array of technologies. Not only will this technology lead to a transformation in the way stakeholders operate, but it will also help them deliver the relevant services or products that customers are coming to expect in today's fast-paced marketplace.

Combining edge and IoT to cut emissions

Moving forward, the demand for sustainability-related services powered by edge computing and IoT will grow in relation to energy efficiency and resource management. This is especially important in the case of environmental monitoring, resource management and supply chain processes. With edge computing, the data from sensors and devices is processed at the edge, where a company's data is being generated. As the data never has to leave the network to provide insights, it helps to reduce latency and puts far less strain on network bandwidth, which ultimately lowers CO^2 emissions.

In fact, a recent report from Vodafone and WPI Economics discovered that emerging technologies such as IoT, 5G and edge computing will help the UK reduce the country's CO^2 emissions by 17.4 million tonnes per year. Whilst these technologies will deliver the efficiency improvements that reduce businesses' carbon footprints, they will not impact society's ability to live, work and travel without significant disruption.

A future of technology convergence

If the past two years have taught us anything, it's that businesses can't prepare for anything. There are some trends that are converging and can help guide them in regard to future plans. Whilst these technologies will help reduce a company's carbon footprint and cut emissions, it also creates opportunities to invest in smart infrastructures and encourage IT leaders to consider investing in 5G to tackle the emerging challenges related to IoT. ■

Don’t let hackers overtake enterprise anti-virus defences

Simon Crocker, senior director - systems engineering, Palo Alto Networks

The sudden surge of remote workers combined with the increased complexity of endpoint attacks is putting pressure on security teams to re-evaluate their approach to enterprise anti-virus. Quite simply, established anti-virus solutions need to be re-imagined and hardened to withstand the sharp rise in attack sophistication and frequency.

When reviewing anti-virus strategies there is an alphabet soup of jargon such as “next-gen antivirus” (NGAV), “endpoint protection platforms” (EPP), and “endpoint detection and response” (EDR).

The reality is that none of these are providing all the specific capabilities needed to protect an enterprise’s endpoints against modern threats.

One thing that doesn’t change is that prevention is the bedrock of cybersecurity. Detection and response to attacks are futile without consistent, coordinated prevention. For example, even the best EDR still detects attacks only after the damage has happened. This puts your security team into a reactive posture, expending operational overhead to understand and assess the attack to then invest even more resources to clean up the damage. In this respect, an EDR is akin to the collision sensor in an airbag that saves lives. This is all very good, but would it not have been better to stop the accident happening in the first place.

So, a better course for modern enterprise anti-virus solutions is a prevention-first approach that deploys the cybersecurity equivalent of both crash avoidance and deterrence.

To achieve this, it is important to understand how attackers currently operate and target endpoints. Many attackers today blend two primary attack methods: targeting application vulnerabilities and deploying malicious files. These methods can be used individually or in various combinations, but are different in nature:

- Exploits are the results of techniques designed to gain access through vulnerabilities in an operating system or application code.
- Malware is a file or code that infects, explores, steals, or conducts virtually any behaviour an attacker wants.
- Ransomware is a subset of malware that holds valuable files or data for ransom, often under encryption, with the attacker holding the decryption key.

When evaluating solutions, the key characteristics to consider are:

1. Malware Analysis

The diversity, volume, and sophistication of threats makes effective threat prevention challenging. There is also the challenge of detecting never-before-seen malware and exploits in addition to identifying known malicious content.

To confront these sophisticated, targeted, and evasive threats, endpoint protection must integrate with shared threat intelligence to learn and evolve its defences. Further, integrating cloud-based threat intelligence with endpoint protection creates deeper analysis to rapidly detect potentially unknown threats. Machine learning on the endpoint should be able to rapidly assess a file to identify suspicious characteristics, as well as perform deeper dynamic analysis and bare metal sandboxing as needed to prevent even more evasive malware.

2. Ransomware Prevention

Ransomware has been around for years but new attacks by groups like REvil have shown that traditional prevention solutions are not enough. Attackers are using much more sophisticated, automated, targeted, and highly evasive techniques. As a consequence, preventing ransomware involves applying a “defence-in-depth” set of capabilities on the endpoint to detect and shut down ransomware in multiple stages of the attack lifecycle.

3. Exploit Prevention

Thousands of new software vulnerabilities and exploits are discovered each year, requiring diligent software patch distribution by software vendors on top of patch management by system and security administrators in every organisation. Addressing vulnerability exploits is the primary reason patches are applied.

Enter Extended Detection and Response (XDR)

To operationalise this approach, it is better to deploy endpoint protection and detection capabilities as features of a holistic extended detection and response (XDR) platform that applies machine learning to a centralised data stream to provide full visibility into attacks across data sources and coordinate prevention across enforcement points.

One key benefit of XDR is how it reduces the pressure on security and network teams. When dealing with cybersecurity, organisations spend a huge amount of time collecting the right security data and making sure it’s in the correct format to use for analytics. They may also need to source data from multiple sources to determine which users, devices, processes, or applications are associated with specific events. XDR automates this through alert stitching—correlating related alerts from different data sources into security incidents—dramatically reducing the volume of disparate alerts analysts must face each day.

With lower alert volume, security teams can move much faster. Leading XDR solutions can close the security coverage gap through seamlessly integrated endpoint protection, detection, and response with a minimal footprint, no dependency on signatures for prevention, a cloud-based management interface, and extensive data collection for event and alert logging. This gives security operations teams the visibility they need for prevention-first operations without negatively affecting endpoint administration.

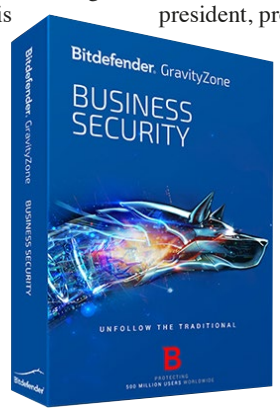
XDR takes prevention capabilities to a higher level than established approaches to enterprise anti-virus. The great advantage of XDR for security teams is how its full-scale visibility and powerful analytics gives them the weapons to fight sophisticated attackers.

PRODUCTS

Bitdefender’s ultimate business solution, **GravityZone Business Security**, is a cost-effective business next-generation anti-virus (NGAV) product.

Designed for SMEs, GravityZone delivers complete protection against all types of malware, be it phishing, zero-day attack, viruses, spyware, ransomware, etc. It uses multiple machine learning techniques, behavioural analysis and continuous monitoring to keep up with the latest threats. Moreover, GravityZone is available in a single platform for all devices, including desktops, laptops, physical and virtual servers.

Earlier this year, Bitdefender unveiled GravityZone XDR, a native XDR solution designed to deliver rich security context, correlation of disparate alerts, out-of-the-box analytics, rapid triage of incidents and attack containment through automated and guided response actions across a business’s complete environment.



“We built GravityZone XDR from the ground-up to help security teams gain a holistic view of their infrastructure, investigate and verify incidents faster, and eliminate threats as they arise,” said Andrei Florescu, senior vice president, products and engineering at Bitdefender. “We placed significant emphasis on security analytics to continuously baseline and adjust detections at runtime to reduce alert fatigue.”

The latest iteration helps maximise team effectiveness, minimise attacker dwell time, enhance threat hunt efficiency, and enable greater cyber resilience.

Malwarebytes Endpoint Detection and Response is an integrated, user-friendly solution for the prevention and detection of attacks with continuous real-time monitoring, isolation and eradication, and can roll-back to a pre-ransomware state.

Malwarebytes features AI-powered next-generation antivirus software, a centralised cloud management console, real-time protection from ransomware, malware, zero-day exploits, and phishing threats. Automated, on-demand security reports, tamper/uninstall prevents, and RDP Brute Force Attack prevention make it one of the few products that doesn’t require a dedicated management team.

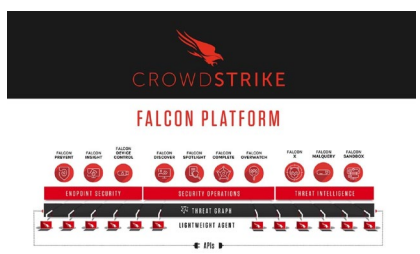
Malwarebytes meets user preferences for a standalone product. It monitors suspicious activity, performs remote threat analysis using cloud-based sandboxing, and offers a simple forensic search across all managed endpoints. For Windows, there is also a Forensic Timeliner which generates forensic system timelines.

CrowdStrike Falcon Endpoint Protection Enterprise offers the only cloud native security platform that has been proven to stop breaches by unifying next-generation antivirus (NGAV) endpoint detection and response (EDR), managed threat hunting, as well as integrated threat intelligence as a single cloud-delivered agent.

The NGAV product provides real-time and historical visibility across endpoints and activities, accelerates investigation and remediation, and ensures that even the stealthiest attacks are always detected. CrowdStrike Falcon Endpoint Protection Enterprise automates complex workflows with Falcon Fusion technology to simplify security operations and accelerate response times.

By using AI, the solution protects against the entire spectrum without requiring daily updates. The best prevention technologies, including machine learning, AI-powered indicators of attack (IOAs), exploit blocking, and high-performance memory scanning, are all incorporated to stop attacks. Endpoints are protected both online and offline.

Intelligent EDR capabilities prevent silent failure by capturing raw events for automatic detection of malicious activity, providing superior visibility, proactive threat hunting and forensic investigation. Entire attacks can be evaluated using the CrowdScore Incident Workbench, which provides context and threat intelligence data.



WithSecure’s business product line, **WithSecure Elements**, promises to deliver an all-in-one security solution with unified endpoint protection across clouds, servers and devices. The easy-to-use system includes vulnerability management, collaboration protection, detection and response, which, the company states, are the only four elements you need to cover the whole security value chain.

WithSecure Elements is compatible with Windows, Mac, Linux, Android and iOS systems, and protects against ransomware, malware, zero-day exploits, phishing attempts, advanced persistent threats, business email compromise (BEC), and brand and domain infringement.

Suitable for enterprises of all size, WithSecure Elements provides complete visibility in a single window, enabling the simultaneous assessment of asset prioritisation, vulnerability identification, incident detection and patch management, among others features. The product collects and analyses data across solutions in real-time, meaning that when a problem is detected in one area, responses are automatically triggered in all solutions. The cloud-native management design enables updates to be handled automatically without further investment in costly servers, thus delivering high levels of protection with low update expenditure.

Despite being extremely easy to use either in-house or via a fully managed subscription, WithSecure also offers to elevate difficult cases to its cybersecurity specialists, which some users may appreciate in the case of advanced threats.

WithSecure claims that the Elements product line - Endpoint Protection, Endpoint Detection and Response, Vulnerability Management - is more resilient to cyber-attacks, achieves less mess and higher efficiency, and less cost with greater simplicity. Each product line is available to purchase separately in order to target a specific weakness, or they can be bundled together for complete protection.

Please meet...

Jed Ayres, chief executive officer, IGEL Technology

What was your big career break?

In 1995, I was studying for an MBA and living in San Francisco when a family friend got in touch. He was the president of AmeriData Technologies, a large computer reseller, and he needed an IT savvy intern for the summer to work on migrating their whole paper-based product catalogue to the Internet and introducing order tracking. The catalogue listed everything they sold like PCs, monitors and peripherals along with pricing. It ran into literally hundreds of pages.

As a courtesy, I went to the interview but turned them down as I really didn't fancy working in their offices in nearby Sacramento. I'd also just got a job at Perry's - one of the coolest bars in town which I thought would be much more fun for a young man new to the big City. He wouldn't let me fob him off though and called back and said, "No isn't the answer, I've got you lodging and you're taking this job". So, I ended up doing both – weekends at the bar and weekdays at AmeriData. I then joined the company as an inside sales rep when I graduated. The business was subsequently sold to GE Capital Services in 1996 and, by aged 24, I was managing a $60 million branch which was the most successful within what became GE Capital's IT Solutions business.

Who was your hero when you were growing up?

My grandfather on my mother's side was a huge influence on me. He spent over 40 years working in the San Francisco education system and was Superintendent of the Middle Schools. Not only that, but he ran one of the largest apple farms in West Sonoma County where he ultimately retired. He was smart and hardworking so I got my work ethic and insight into leadership from him. He taught me nothing great is done alone and always about building, empowering and recognizing the team you're working with.

What would you do with £1m?

I'd invest in tiny homes and create a community of them. In the USA, we have a housing crisis like the UK and need a lot more affordable places for people to live. So, tiny homes are all about quickly manufacturing low-cost buildings in a factory to a high specification which is much more environmentally sound and sustainable than building onsite. I'd then want to use solar panels or ground or air source heat pumps for power to reduce carbon emissions.

Where would you live if money was no object?

Honestly, I love where I live which is in the Mount Tamilpais area of Marin County – famous as this is where mountain bikes were invented. It's north of the Golden Gate Bridge on highway 101. My backyard is 46,000 acres of open protected public space.

Which law would you most like to change?

America has a problem with guns and pretty much anyone can buy one, even high-powered assault rifles with a magazine. There are just too many in circulation and too many deaths. My 14 year old son has to have active shooter drills at school which is shocking. We have to do better. That means changing the law and using technology to register and track guns and their owners more stringently.

The Beatles or the Rolling Stones?

It has to be the Rolling Stones. Why? They're still rolling after 60 years! They're also the first famous rock band I saw in the early 1990s when they played at the Oakland Coliseum stadium.

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

I'd love to meet Barack Obama. He's someone with incredible intellect, he's a great orator and leader and came to the presidency through a different route to most, starting out as a community organizer in Chicago before going into law. He's a similar age to me and loves basketball – which I do too – so I'm sure we'd have a lot to talk about. I'd take him to International Smoke, a restaurant near IGEL's offices which serves wood-fired steaks, ribs and seafood. It's part owned by Ayesha Curry, the wife of the National Basketball Association mega star, Steph Curry, who's scored the most 3-point field goals in NBA history at 3,117.

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

My mother once said to me, "Leave things better than you found them." I've always tried to do that in relationships, in business and with friends and family. Living by that maxim, you're always looking to help others and the world at large, what we at IGEL call a 'servant heart.'

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

Hospitality. I love being around and serving people. I actually took a four-year sabbatical away from the IT industry - between 2002 to 2005 - and bought a hotel/restaurant called McCallum House in Mendocino on the northern coast of California, my hometown. There's a story here, too. When I was 15, I got my first job there as dishwasher. Twenty years later, I bought the business and the chef that hired me was still there and became an employee which was wonderful. ■