ComputerWeekly

22-28 NOVEMBER 2022

Scammers target World Cup

Cyber criminals have football fans in their sights as tournament kicks off

NATTAWIT/ADOBE

TechTarget ComputerWeekly.com

Team working on Horizon EPOSS was the 'joke of the building'

The ICL team working on the Post Office Horizon IT system lacked experienced developers and used bad software development practices, a former employee told the public inquiry into the scandal. Software developer David McDonnell said it was clear the critical cash account component of the software, which enables subpostmasters to balance their accounts, should have been rewritten.

SAP Build launched to appeal to business user developers

SAP has launched a low-code application platform aimed at business users, dubbed SAP Build. Julia White, chief marketing officer for SAP, said the next wave of "business transformation" would be driven by business users whose expertise has so far been untapped, especially when identifying opportunities for business process automation. Build is part of the supplier's Business Technology Platform.

HMRC to migrate from Government Gateway to One Login in 2023

HM Revenue & Customs (HMRC) will begin migrating to the government's One Login digital identity platform next summer. HMRC chief technology and design officer Tom Skalycz said this will mean transferring services away from Government Gateway, the department's identity, authentication and transaction platform. The One Login for Government programme has the objective of simplifying access to central government.

Tech commoditisation a problem, says NHS Digital interim CEO

Too many technology systems are being used across the NHS, according to NHS Digital interim CEO Simon Bolton. He said the NHS needs to get to grip with the number of systems in use and the variability this brings to patient care. Bolton said that since joining the NHS, he has been "struck" by the "absolute spectrum of technology solutions that we've got to fix the same problems".

TEROVESALAINEN/ADOBE

Online shopping scam victims lose average of £1,000 per person

UK-based victims of online shopping scams lost an average of £1,000 each during the 2021 holiday season, according to National Fraud Intelligence Bureau statistics released to coincide with a new National Cyber Security Centre anti-fraud campaign, run under the auspices of its Cyber Aware programme. UK shoppers lost more than £15m to cyber criminals from November 2021 to January 2022.

›Catch up with the latest IT news online.

Women more likely to leave tech jobs than men

Women are more likely to leave their roles in the technology sector than men, according to research by InnovateHer, which found 45% more women than men leave technology roles, and half of the women in tech roles leave before the age of 35.

Defra confirms final settlement over 'historic' IR35 errors

The Department for Environment, Food and Rural Affairs (Defra) has handed over a further £23m in unpaid tax to HM Revenue & Customs for IR35-related compliance errors – sending its final settlement figure soaring to £86.5m.

Sadiq Khan launches Data for London Advisory Board

London's mayor has launched an advisory board to help coordinate the collection, sharing and use of data for public benefit across the capital. The board will help coordinate effective and responsible data sharing.

17 West Midlands NHS trusts deploy digital pathology

Some 17 NHS trusts across the West Midlands have gone live with a digital pathology system aimed at improving cancer diagnosis. The programme is thought to be one of the largest in Europe and covers four NHS pathology networks.

MoD recruits Immersive Labs to bolster cyber resilience

The Ministry of Defence (MoD) is to deploy a package of offerings from security specialist Immersive Labs to upskill existing individuals and teams to confront threats, prove their cyber readiness and identify talent to fill open roles.

G-Cloud 13 launch hits shaky start with missing functionality

The government's Crown Commercial Service has assured the public sector IT buying community that the apparent removal of the supplier transparency function from the G-Cloud 13 framework is temporary. ■

Microsoft CEO outlines 'digital imperatives'

Microsoft CEO Satya Nadella has outlined key digital imperatives that will help organisations to tackle global challenges such as the transition to new energy sources and the inequities that exist in the world today, including the shift to cloud, leveraging data and artificial intelligence, and cyber security.

FABRICE COFFRINI/GETTY

› *Agility, business more important than cost for IT teams.*
› *Scottish government to pilot digital identity platform.*
› *5G gains pace as Vodafone faces off H1 headwinds.*
› *Another Log4Shell warning after attack on US.*

› *Catch up with the latest IT news online.*

Cracking the code for a modern approach to enterprise software development

Overworked IT departments need a better way to deliver digitally enabled products and services at the speed that the business requires. Cliff Saran *reports from the Gartner Symposium in Barcelona*

By 2024, 80% of technology products and services will be built by people who are not full-time technical professionals. This was one of the findings revealed by Gartner at its annual Symposium in Barcelona.

Combined with robotic process automation (RPA) and the concept of composable business, in which teams across IT and the business implement composable applications, on the takeaway menu at the Gartner Symposium was the fact that CIOs may need to rethink how and where they allocate resources to support digital business initiatives.

In a presentation entitled *The new economics of technology*, Gartner distinguished analyst Daryl Plummer asked delegates to consider what the notion of writing code meant to them. He said: "Is it about writing code or is it something else?"

Low-code and no-code tooling makes it easy enough for almost anyone to "program", which, said Plummer, means the business needs to distinguish between tasks that can be achieved by workers using such tooling and where specialist developers are needed.

Using eBay as an example, Plummer suggested that low code and no code could now be regarded as part of normal work activity. On eBay, for instance, although it provides a site for auctions, all of the actual work – from uploading images of products to writing descriptions and postage – are tasks that eBay customers do for themselves.

This is the concept of "bring your own" application and data analytics, in which employees take on responsibility for creating applications and the analytics needed to do their work, he said. Professional developers are then free to develop the IT integration and governance required to support this environment.

Such a policy on application development may offer IT leaders a way to combat the ever-growing IT skills crisis and work backlog brought on by the business's appetite for digitisation, artificial intelligence and RPA.

Manufacturer Dyson is a customer of low-code tools provider Mendix. It has used Mendix to develop native web and mobile applications, which can be used at the point of manufacturing or in a distribution centre. Discussing the opportunities of low-code tools, Tom Wilmot, strategy transformation manager at Dyson, said: "Low code is a fantastic capability for making business react in a secure and safe environment. It enables us to work with IT in a way that we do safely without a full project lifecycle."

Gartner's Magic Quadrant report for low-code tools, published in September 2021, forecast that by 2025, 70% of new applications developed by enterprises will use low-code or no-code technologies – up from less than 25% in 2020. Gartner reported that, on average, 41% of employees in an organisation are business technologists. These are employees who report outside of IT departments and create technology or analytics capabilities for internal or external business use.

Nightmare of unmanaged applications

Although all of this is positive news for overworked IT departments, there is a huge risk that low code could open businesses to a nightmare of unmanaged applications. This happened with Excel macros, where people developed neat spreadsheet automation tricks that became embedded in business processes. But if the person who originally developed the macro leaves the business, because the script is undocumented, no one in IT is aware of the macro or how it works.

Given the potential benefits that low-code tools offer in terms of enabling people in the organisation to develop their own software to improve the efficiency of the business processes with which they interact, the industry is recognising the massive risk that this practice poses.

```
        return ( elem === document.activeElement ) === ( type === "focus" );
function on( elem, types, selector, data, fn, one ) {
    var origFn, type;

    // Types can be a map of types/handlers
    if ( typeof types === "object" ) {
        // ( types-Object, selector, data )
        if ( typeof selector !== "string" ) {
            // ( types-Object, data )
            data = data || selector;
            selector = undefined;
        }
        for ( type in types ) {
            on( elem, type, selector, data, types[ type ], one );
        }
        return elem;
    }

    if ( data == null && fn == null ) {
```

Gartner has forecast that by 2025, 70% of new applications developed by enterprises will use low-code or no-code technologies

SONG_ABOUT_SUMMER/ADOBE

Dyson's Wilmot said his business has concentrated on operational excellence focused on project audits, adding that people and the process around low-code development are crucial. He suggested that CIOs should decide: "Who will be your core low-code coders in IT and in the business?"

Wilmot also urged CIOs considering the idea of opening up low-code development to business users who would like to code, to ensure that processes are in place to prevent the code they develop from "running wild".

Clearly there are numerous opportunities to improve on how things work, especially in organisations that have grown organically over time, where, to achieve a business objective, employees need to use numerous systems that don't talk to each other. More often than not, data has to be rekeyed, which is both error-prone and labour-intensive.

Hyper-automation

Gartner sees low code as a key component of hyper-automation, which it defines as orchestration using multiple technologies, tools or platforms. Such orchestration offers a way to integrate disparate systems that eliminates, or cuts back on, the level of manual intervention required. Research for its Magic Quadrant report found that 13% of business technologists say low-code development tools are among the three most-used tools (based on frequency and volume) to support automation initiatives.

For instance, Santander, a Blue Prism customer, has used RPA on a number of projects to save 625 hours of work. Piotr Wyrzykowski, IT area lead at Santander Bank Polska, said the bank had run a discovery process to identify projects suitable for automation, one of which involved customer complaints. By using RPA, he said, Santander reduced the complaints-handling process from two days to two hours.

Santander is also using RPA to integrate its services, which can then be offered through partner financial institutes to fulfil customer banking needs using the bank's products and services.

> "Low code is a fantastic capability for making business react in a secure environment"
>
> Tom Wilmot, Dyson

These technologies can be tied together in an overall strategy for digitally empowering the business. Gartner uses the term "composable business" to describe a business organised, from a digital technology perspective, into distinct blocks of application functionality designed for easy configurability to meet ever-changing business requirements.

According to Gartner, organisations are adopting application composition technologies that enable teams that combine business and IT people to implement composable applications.

Low-code application platforms are one of the key technologies that drive greater composability of application services, functionality and capabilities. ■

› Software that powers finance departments can help navigate the economic crisis.

Cyber criminals have World Cup Qatar in their sights as tournament kicks off

Malicious cyber activity around the FIFA World Cup was ticking upwards even before Sunday's opening game, with threats likely to present themselves in great numbers and many forms throughout the event. Alex Scroxton reports

The FIFA World Cup Qatar 2022 has kicked off, and while the tournament is surrounded by controversy over the host country's human rights record, among other things, it is attracting massive attention from all over the world, with a TV audience expected to number well into the billions.

Inevitably, the World Cup is also attracting the attention of cyber criminals and other threat actors who, as has been seen time and time again, are adept at appropriating significant events and incorporating them into their campaigns.

The Digital Shadows Photon research team has been tracking cyber threats coalescing around the World Cup over the past few months using a specially created alert system. It has found that broadly, threats to the event can be arranged into four categories – brand protection, cyber threat, physical protection and data leaks. Of these, most of the observed activity relates to the cyber threat category.

"Scams could present themselves in many forms," the Photon team wrote in an online advisory. "For instance, financially

FRANCOIS NEL/GETTY

motivated threat actors often plant in malicious URLs spoofing these events to fraudulent sites, hoping to maximise their chances of scamming naive internet users for a quick, illicit, profit.

"At the same time, hacktivist groups may exploit the public attention given to such events to exponentially increase the reach of their messages. State-sponsored advanced persistent threat (APT) groups may also decide to target global sporting events to achieve state goals to the hosting country or the broader event community."

Hundreds of threats

In the course of its research, the Photon team encountered hundreds of online threats, many of which are clearly set up to target the general public, exploiting their anticipation and excitement, and their desire for more information about the World Cup, to lure them in.

Among the team's discoveries were more than 170 domains impersonating official World Cup online properties, many of them phishing websites intended to steal their victims' data; 53 malicious mobile apps, used to install adware, steal data and credentials, and download additional malware payloads; and dozens of fraudulent social media pages, some of them being used to spread dubious affiliate marketing or pyramid scams.

Countering such threats is, in general, a matter of remaining vigilant to the signs of a scam, not clicking on links in unsolicited emails, downloading apps only from the App Store or Google Play, and seeking news and information from known, trusted media, such as the BBC or Sky.

It is always also worth bearing in mind the adage that if an offer seems too good to be true, it probably is. Further guidance for consumers is available from the National Cyber Security Centre.

The Photon team also pointed to the possibility of more sophisticated cyber activity around the World Cup. For example, during its research, the team found multiple advertisements for raw data logs that had been stolen using the Redline malware. Redline is an infostealer used to gather credential pairs, autocomplete data and credit card information from its victims' web browsers. It can also harvest other technical data about the compromised system.

Researchers encountered hundreds of online threats, many of which are clearly set up to target the general public, exploiting their excitement about the World Cup to lure them in

Some of these data logs appear to relate to World Cup assets. Such information could be used to take over victims' accounts and conduct further malicious activity.

FIFA WORLD CUP · Qatar2022™
FIFA WORLD CUP · Qatar2022™
FIFA WORLD CUP · Qatar2022™
FIFA WORLD C
FIFA WORLD CUP ·
FIFA WORLD CUP · Qa

ADRIAN DENNIS/GETTY

The team also turned up some evidence that suggests more high-level, targeted activity may hit organisations involved in the tournament, such as sponsors, national teams, or organising bodies in Qatar, which may be targeted for disruptive, human-operated ransomware attacks. Lockbit – probably the most active ransomware cartel at the time of writing – is known to have attacked organisations located in Qatar.

Hacktivists might strike

No less impactful, and perhaps more so given their frequent courting of global media, is the possibility of hacktivist activity, which has been on the up and up during 2022, with groups such as Ukraine's IT Army facing off against the likes of the pro-Moscow KillNet collective. For example, Anonymous, already globally renowned for its hacktivist campaigns, appears to have the World Cup in its sights. On 25 October, a group representative called on FIFA to ban the Iranian national squad in the light of Tehran's brutal crackdown on anti-regime protests, signing off with the Anonymous group's now traditional salutation, "Expect us".

"Given the high level of activity carried out by hacktivist groups in 2022, it is realistically possible that said groups will target the 2022 Qatar World Cup to some extent," said the Photon team. "Hacktivist groups could target the organisers or the sponsors of the tournament, and may do so using DDoS [distributed denial of service], defacement or data destruction attacks." ■

INTERVIEW

Kyiv is ready for anything

Karl Flinders talks to Kyiv City Council's CIO and deputy CIO about the challenges of war

#KYIVDIGITAL

Oleg Polovynko, Kyiv City Council: "Our challenge is to manage the population and make their lives safer"

Turning a transport booking service into an air raid alert system is not the typical task of a CIO, but that is what the IT team at Kyiv City Council was forced to do in the early days of Russia's invasion of Ukraine.

When Russian tanks entered Ukraine in February and missiles rained down on cities, the IT team at Kyiv City Council embarked on an innovation journey born of necessity. Its response to the war has given the team an experience like no other.

Oleg Polovynko, CIO at Kyiv City Council, tells Computer Weekly that the challenges it was solving had a strong connection with citizens. "This is our reality now, and our challenge is to manage the population and make their lives safer and of a better quality," he says. "All our solutions are creating a fast and trusted way of communicating with citizens because any shit can happen, whether it's an epidemic, a war, or a natural disaster."

Polovynko says the safety of citizens came first, and to this end, the Kyiv Council IT team's first job when the war started was to quickly develop a method of warning people when missiles were heading in their direction. Through the pre-existing Kyiv Digital mobile app, which was launched in January 2021, the team adapted an existing transport information service to send air raid warnings to citizens. At the time, although Kyiv had a public alert siren, it covered only about 30% of the city.

Deputy CIO Victoria Itskovych says the service it adapted to warn citizens of air raids was originally a transport application offering ticketing, parking and municipal information services.

"After the war started, we had to quickly change this app into an air raid alert system," she says. "All municipal transport stopped

HOME

in the early days and weeks of the war, and the main goal was to provide notifications and warnings of missile attacks.

"The transport information service already had the notification functionality, but the problem was that it wasn't designed to send notifications to the entire user base of millions of people." The team made the changes and had the system up and running in a matter of hours.

This was the first service launched in wartime by the team, but more soon followed, as people needed help with the basics of life. "After the air raid notification service, we launched other services in the app, including giving information about where people could safely buy food and pharmaceuticals," says Itskovych.

When the war started, everything closed. Then stores reopened slowly, often only for a couple of hours a day, and there was no source of information on what was open at what time, she says. "We launched a channel with up-to-date information integrated with a map. After the pharmacies, we launched a service for buying food, accessing water sources, medical centres, petrol stations, and so on – the basics of life."

Service for SMEs

The next project saw a service developed for small businesses which, for safety reasons, had to suddenly close after the invasion. "We launched a campaign for SMEs that were going to open and put them on a map telling people they were open," says Itskovych. "This was a great success."

She says this was always intended to be a temporary service and people are now returning to Google Maps for information. "This service is coming to an end now, but in the first months it was rather essential," she adds.

> "We made a platform where people hiding in shelters could leave their request for connectivity and internet providers would offer services"
> Victoria Itskovych, Kyiv City Council

Another essential in today's world is internet connectivity. In the early months of the war, the City Council also developed a service to ensure people had connectivity in air raid shelters, known as Wi-Fi in Shelters. "People who did not leave Kyiv were forced to hide in shelters, which are normally under buildings, with no connectivity," says Itskovych. "We made a platform where people hiding in shelters could leave their request for connectivity and internet providers would offer services."

The requester and provider connection platform covered 815 shelters in the early months of the war. Telecoms companies offered the service free of charge, allowing people to send messages to family and friends to let them know they were safe.

In the early days of the conflict, about 40 people were working on IT for the City Council. "One of the main challenges was the safety of our people," says Itskovych. "Most live in the Kyiv region, which was occupied early in the war, and many could not work."

Before the Russian invasion, Kyiv City Council was already on a journey to digitise its services and work to create a smart city had begun with the transport information and booking system. The app also offered e-democracy services, such as giving people a say in how money is spent on projects in the city, known as a participatory budget.

The participatory budget sees money set aside for proposed budgets, which citizens then vote on to see which receives funding. "This is within the Kyiv Digital app, and although it is on hold during the war, it has been very successful," says Itskovych.

E-petitions are another part of the city's digital push. "Of course, petitions were there before, but by integrating them in Kyiv Digital, we made them available to all citizens. It is easier now and there are more petitions," she adds.

Improve citizens' lives

For the future, CIO Polovynko says Kyiv City Council wants to take what it has learned to help improve citizens' lives. "We want quality feedback and we want to give more power and provide more solutions to what people need," he says.

This includes as many channels for people to communicate their needs with the City Council as possible, such as through e-petitions and participatory budgets. "Our goal is for 100% of services to be electronic," says Polovynko.

This goal is aided by another major project, known as Diia. The Diia App is a national project for the whole of Ukraine. Launched in October 2020 by the Ministry of Digitalisation, it provides electronic documents such as driving licences, passports, Covid tests

Oleg Polovynko and Victoria Itskovych have led their IT team on an innovation journey born of necessity since the Russian invasion

#KYIVDIGITAL

MISU/ADOBE

Kyiv has endured considerable damage since the war began

and birth certificates on people's smartphones. Currently, about 16 million people use the app, which has helped people displaced by the war access their documents.

One thing that wasn't known to the Kyiv IT team but did increase when Russia invaded is state-sponsored cyber attacks. "You have the same war in cyber as you do in the physical world," says Itskovych. "Massive cyber attacks were launched just before the invasion because the Russians wanted to make a mess of our cyber infrastructure so we would be so busy fixing it, we wouldn't notice hacks. One thing that saved us was a heterogeneous infrastructure. We didn't have any data leakage, with none stolen."

But she says some less essential municipal systems were deliberately shut down to enable teams to focus on keeping essential systems running. "When your country is attacked, you don't need all your services, so we temporarily shut down some services that were not required so we could strengthen them and increase our security," says Itskovych.

The Russian attack has seen the IT community in the Ukraine come together to support the war effort. "From the first day of the war, IT professionals here in Ukraine started in small groups trying to do something," says Itskovych. "We had the IT Army, which was created as a brand for IT professionals who wanted to help defend the country. After the war, we will be stronger, because when you are under stress, you become stronger. After we win, we will see a giant boost in technology and will have a lot of work to rebuild. We need money, but we can't rely on other countries for ever, so we need to produce. IT can be one of our main exports. IT was already a noticeable part of our exports, but this will increase." ■.

ComputerWeekly

Computer Weekly,
10 Exchange Square,
9th Floor (West),
London EC2A 2BR

Telephone: 020 7186 1400

Editor in chief: Bryan Glick
bglick@techtarget.com

Managing editor (technology): Cliff Saran
csaran@techtarget.com

Investigations editor: Bill Goodwin
wgoodwin@techtarget.com

Senior editor, EMEA: Karl Flinders
kflinders@techtarget.com

Senior editor, UK: Caroline Donnelly
cdonnelly@techtarget.com

Security editor: Alex Scroxton
ascroxton@techtarget.com

Networking editor: Joe O'Halloran
johalloran@techtarget.com

Management editor: Lis Evenstad
levenstad@techtarget.com

Storage editor: Antony Adshead
aadshead@techtarget.com

Business applications editor: Brian McKenna
bmckenna@techtarget.com

Business editor: Clare McDonald
cmcdonald@techtarget.com

Senior reporter: Sebastian Klovig Skelton
sklovigskelton@techtarget.com

Production editor: Claire Cormack
ccormack@techtarget.com

Senior sub-editor: Bob Wells
rwells@techtarget.com

Senior sub-editor: Jaime Lee Daniels
jdaniels@techtarget.com

Senior sub-editor: Ryan Priest
rpriest@techtarget.com

Vice-president of sales, EMEA: Jat Hayer
07557 433681 | jhayer@techtarget.com

TechTarget

Smart energy needs intelligent strategy

In October, electric vehicle (EV) charger manufacturer Andersen went into administration. These devices are supposedly smart – they communicate with servers and, in the future, will offer a way for the electricity grid to balance usage of EV charging, based on electricity demand. The company has found a saviour, EVios, which has announced its intention to acquire Andersen. Crisis over. Well, not really. Andersen's demise raises important questions on the viability of the services startups build around their products. If a buyer had not been found, what would have happened to Andersen's existing customers and the smart charging software they rely on?

In July 2021, NCC Group published an article discussing the risks of cloud software. It said that if a supplier defaults in its service obligations, pulls the plug or goes insolvent, its customer loses access to the software. Even if the application code is available via a cloud escrow arrangement, NCC said the provider's customers would probably have difficulty deploying and managing the app because they have only ever experienced it as a user.

While NCC focused on the professional software buyer, consumers are unwittingly buying cloud-based software-powered services when they purchase smart products. A smart speaker or doorbell is only useful when it is connected to a service. Without it, the device is just a powered brick, which is what happens when an Amazon Echo loses its internet connection. Such devices may be considered "disposable" and can be replaced, without major disruption, with one from another provider. But the same is not true of smart EV chargers, heat pumps, PV batteries and smart heating systems, which offer a way to manage energy consumption and lower our reliance on fossil fuels for heating and hot water.

HOW MANY MORE SMART ENERGY TECH STARTUPS WILL GO TO THE WALL?

Among the discussion topics coming out of the 2022 United Nations Climate Change Conference (COP27) is the idea of using innovation and technology to transition to low-carbon energy systems. Cumulatively, every smart energy device we install in our homes and businesses plays a small part in helping the UK meet its Paris Agreement commitments to lower greenhouse gas emissions by 2030.

Andersen was founded only in 2015, but ran out of money due to supply chain issues in the automotive sector. How many more smart energy tech startups will go to the wall by 2030? We can't rely on bailouts from interested businesses to support the customers of those that fail. We need a strategy to maintain and support smart energy firms' innovations long after they have ceased to exist. ■

Cliff Saran, managing editor (technology)

› Read the latest Computer Weekly blogs.

BUYER'S GUIDE TO ANTI-RANSOMWARE | PART 2 OF 3

How to defend your data (and finances)

Stephen Pritchard looks at the impact of ransomware on storage and backup, how storage and data protection can best be used to combat ransomware, and how they fit in the fight against it

UTHAWUT/ADOBE

HOME

In the past decade, ransomware has gone from being a relatively obscure crime to a multibillion-dollar industry, with the largest enterprises and even governments in its sights.

Organised cyber crime groups demand ransoms of six and seven figures or more from their victims. Using a combination of network infiltration, malware and cryptography, ransomware locks firms out of their data by attacking storage, encrypting data and even disabling backups.

Cyber crime groups have also been boosted by the growth of cryptocurrencies, which give criminals a low-risk way to extract payouts, and by techniques that go beyond data encryption. These include double- and triple-extortion attacks and threats to release sensitive data.

Ransomware attacks such as those that hit Maersk, Colonial Pipeline and the Irish Heath Services Executive have dominated headlines because of the disruption they caused. But ransomware attacks are now commonplace, and increasingly hard to prevent. According to experts at data security company Kroll, between 25% and 45% of the firm's investigations currently involve ransomware attacks.

Laurie Iacono, associate managing director covering threat intelligence at Kroll, says a small number of ransomware groups are now behind most attacks, and as many as 86% of attacks now involve data exfiltration – not just encryption. "What we see is that ransomware has become a predominant attack vector," she says.

How do ransomware attacks work?

The conventional path for ransomware into an organisation is through an infected attachment that contains an executable file, or by conning users into visiting a website that contains malware. That injected software deploys on the network and seeks out its targets.

Double- and triple-extortion attacks create backdoors into systems that allow the attackers to exfiltrate data. Increasingly, this goes hand in hand with disabling backups and attacks on core network services such as Microsoft Active Directory.

The latest generation of ransomware attacks target backup systems, appliances and virtual machines. "They are targeting physical appliances and virtualised appliances," says Oisin Fouere, head of cyber incident response at consulting firm KPMG. "A lot of backup systems are hosted on virtual infrastructure. They have started targeting and deleting operating system-level information on those systems, as well as going after the bare bones of the systems."

And as Kroll's Iacono points out, ransomware groups often recruit people with technical knowledge of backup systems.

But first, the ransomware has to enter the corporate network. The conventional – and still most common – approach is to use a phishing attack or other form of social engineering to deliver infected attachments or convince employees to click on infected web links.

> "OFTEN, A PHISHING ATTACK OR RANSOM ATTACK CAN BE USED AS A MASKING TECHNIQUE FOR SOMETHING ELSE THAT IS GOING ON, OR CAN BE MASKED BY DOING SOMETHING ELSE"
>
> KEITH CHAPPELL, PA CONSULTING

During the Covid-19 lockdowns, ransomware groups exploited weaknesses in virtual private networks and remote desktop systems, which caused a spike in ransomware cases. "There was a lot of exposure around poorly protected or inadequately configured remote access systems, which meant attackers didn't need to spend time trying to solve the intrusion vector problem," says KPMG's Fouere. "They were almost being presented with a front-door-left-open scenario, and that was a favourite choice over the past couple of years."

The hardening of these access points is behind a recent fall in ransomware incidents – but this is no cause for complacency, experts warn. Keith Chappell, a cyber security expert at PA Consulting, says we are seeing "more deliberate, more targeted and better-researched attacks that actually have a purpose, be that to disrupt operations or to extort to make money".

How does a ransomware attack affect storage and backup?

Ransomware attacks set out to deny access to data. Early-generation attacks targeted disk drives, often on individuals' PCs, with fairly low-grade encryption methods. Victims could obtain a decryption code for a few hundred dollars.

However, modern attacks are both more selective and more damaging. Attackers increasingly use reconnaissance to find high-value targets. These include personally identifiable data, such as customer, commercial or health records, or intellectual property. These are the files firms will most fear being made public.

But attackers also target networks and identity and access management data, operational systems, including operational technology, and live data flows, as well as backups and archives. Double- and triple-extortion attacks that go after backups or disaster recovery and business continuity systems offer the greatest chance of a payout. Without the ability to recover a system or restore data from backups, firms may have little choice but to pay up.

Attackers also look for accounts they can compromise and use to escalate privileges to carry out further, or deeper attacks. Security teams need to secure not just main data stores, but also administrative systems. "Very often, a phishing attack or ransom attack can be used as a masking technique for something else that is going on, or can be masked by doing something else," says PA Consulting's Chappell.

How do storage and backup help in case of a ransomware attack?

Even though criminal hackers actively target backups, these remain the best defence against ransomware.

Firms need to ensure they take regular backups and that these are immutable, stored off-site, or ideally, both. "You should be backing up data daily, weekly and monthly, and you should be

Ransomware attacks have become commonplace and are increasingly hard to prevent

ARTINSPIRING/ADOBE

storing backups in physically separate, disconnected locations, ideally in different formats," says Chappell.

Much has been said about the need to "air gap" data from systems that might be attacked, and nowhere is this more important than for storing backup copies. However, older backup media, such as tape, are often too slow to allow a full recovery in the timescales the business demands. "Organisations realised they can't wait several months for these tape backups to restore," says KPMG's Fouere. Instead, clients are looking at cloud-based resilience and recovery, primarily for speed, he says.

In turn, backup suppliers and cloud service providers now offer immutable backups as an extra layer of protection. High-end, active-to-active business continuity systems remain vulnerable to ransomware as data is copied from the primary to the backup system. So, firms need solid backup and ways to scan volumes for malware before they are used for recovery, and ideally as data is being saved.

But IT organisations also need to take steps to protect backup systems themselves. "They are vulnerable, too, just like any other software product is," says Kroll's Iacono. "You have to make sure that backup systems are patched. We have had cases where threat actors leverage vulnerabilities in backup systems to help them with data exfiltration or to evade detection."

FIRMS NEED SOLID BACKUP AND WAYS TO SCAN VOLUMES FOR MALWARE BEFORE THEY ARE USED FOR RECOVERY, AND IDEALLY AS DATA IS BEING SAVED

Some IT teams are going even further. With ransomware groups spending more time on reconnaissance, firms are obscuring the names of servers and storage volumes. This is a simple, low-cost step to avoid using obvious labels for high-value data stores, and it might buy valuable time when it comes to shutting down an attack.

What are the limits of storage and backup as protection against ransomware?

Good discipline around data backups has reduced the effectiveness of ransomware attacks. This may explain why cyber crime groups have moved to double- and triple-extortion attacks, targeting backup systems and exfiltrating data.

Using immutable backups alongside disk or cloud storage still minimises the impact of ransomware. But firms need to ensure that all parts of critical systems are fully protected – and this includes testing. Even if the main data store is backed up, a system can fail to restore if operational or administration data is encrypted because they have been left off the backup plan.

Firms also need to allow for data restoration where good backups do exist. Even with the latest backup and recovery tools, this is still a disruptive process.

Also, immutable backups will not prevent data exfiltration. In this case, firms need to invest in the encryption of data assets. However, they can only do this if they have an accurate, up-to-date understanding of where their data is. To achieve this, organisations should look at monitoring tools that can detect unusual data movements and invest in protecting privileged user accounts.

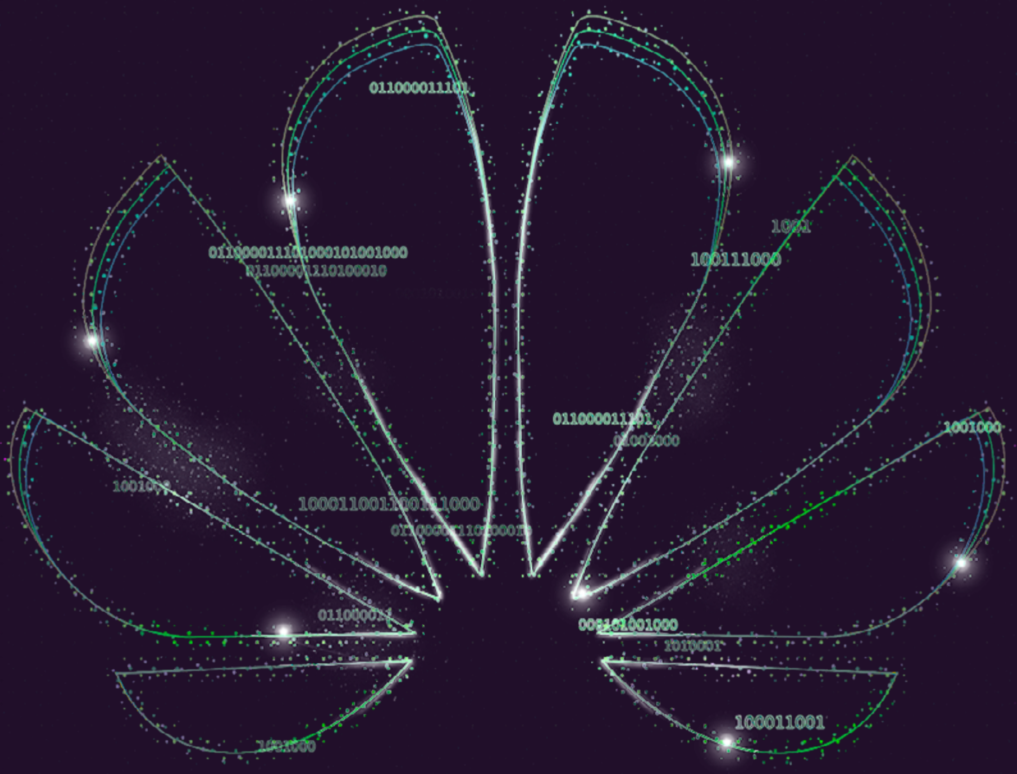
With most ransomware still spread by phishing and social engineering, businesses can take technical steps to protect their perimeter. But training staff to spot suspicious emails, links and attachments, coupled with multifactor authentication, are the strongest defence against ransomware. For ransomware, as with other forms of fraud and online crime, security awareness is an essential part of defence in depth. ■

MARTIALRED/ADOBE

Double- and triple-extortion attacks that go after backups or disaster recovery and business continuity systems offer the greatest chance of a payout

SUSTAINABILITY

Huawei sets out its stall for a data-rich world



Maxwell Cooter looks at how Huawei is setting out to cope with the data strains put on organisations, while mitigating the environmental impact

JDANIELS

HOME

It has become a truism that data is the driver for businesses. We have all heard the clichés about data becoming the new oil and how companies should be making the most of all the available data they have as it will lead to untold riches, and so on.

But there has been one big problem with this vision: organisations have been struggling to keep up with the storage required to keep pace with demands on data. And it's a problem that's not going away any time soon.

However, to compound the difficulties that businesses are facing, there is another issue to consider: the environmental impact of this process of transformation. Datacentres already contribute greatly to carbon dioxide emissions – about 2%, the same as the airline industry – and any further increase could lead to more CO_2 at a time when organisations are trying to reduce their carbon footprints.

IT and networking technology giant Huawei is looking at a new way of exploring these issues and trying to fathom how to do more to meet these new demands. At its recent Innovative Data Infrastructure forum, the company set out its plans to both cope with the new strains put on organisations, while mitigating the environmental impact.

Decoupled systems

Huawei laid out some of the ways that it was looking towards the future. The company has announced a different approach to storage by prioritising "the development of decoupled storage-compute architectures and diverse data application acceleration engines", said Peter Zhou, president of Huawei's IT product line.

Zhou believes that although Huawei has already offered a range of storage options, there is a need to keep up with this tidal wave of data, and existing products cannot handle these demands efficiently. "We are ushering in the yottabyte era," he said. "Data applications are growing faster than ever."

Zhou spoke of the inexorable rise of cloud computing and how it is leading to a slowdown in the take-up of hard disk drives (HDDs) and a rise in flash memory. There has clearly been a rise in data demand: talk of a yottabyte (YB) era is no exaggeration. According to Huawei's own *Global industry vision report*, by 2030, 1YB of data will be generated globally every year – 23 times the amount in 2020 – a whopping increase in just a decade.

Organisations are struggling to cope with this increase and Huawei thinks its approach will make some headway in tackling this. By decoupling storage, organisations can be more granular in their approach to data, ensuring that applications that are data-intensive can be handled efficiently, while the rest can be archived. This leads to a better use of resources and more efficient processing.

It is a far cry from the traditional data warehouses, where compute and storage are tightly integrated – an approach that has been adequate for the type of corporate applications in the past, but can't keep pace with the analytics-intensive demands of the modern corporate.

However, according to Huawei, there are four areas that need to be looked at to make this vision work – all areas in which the company believes it has the answers.

Economic use of data

First of all, there is the lack of products that can handle the new generation of applications. Companies are turning to emerging technologies such as distributed databases, big data, artificial intelligence (AI) and high-performance data analytics (HPDA) applications, and need to find a way to handle them.

> According to Huawei's own *Global industry vision report*, by 2030, 1YB of data will be generated globally every year – 23 times the amount in 2020

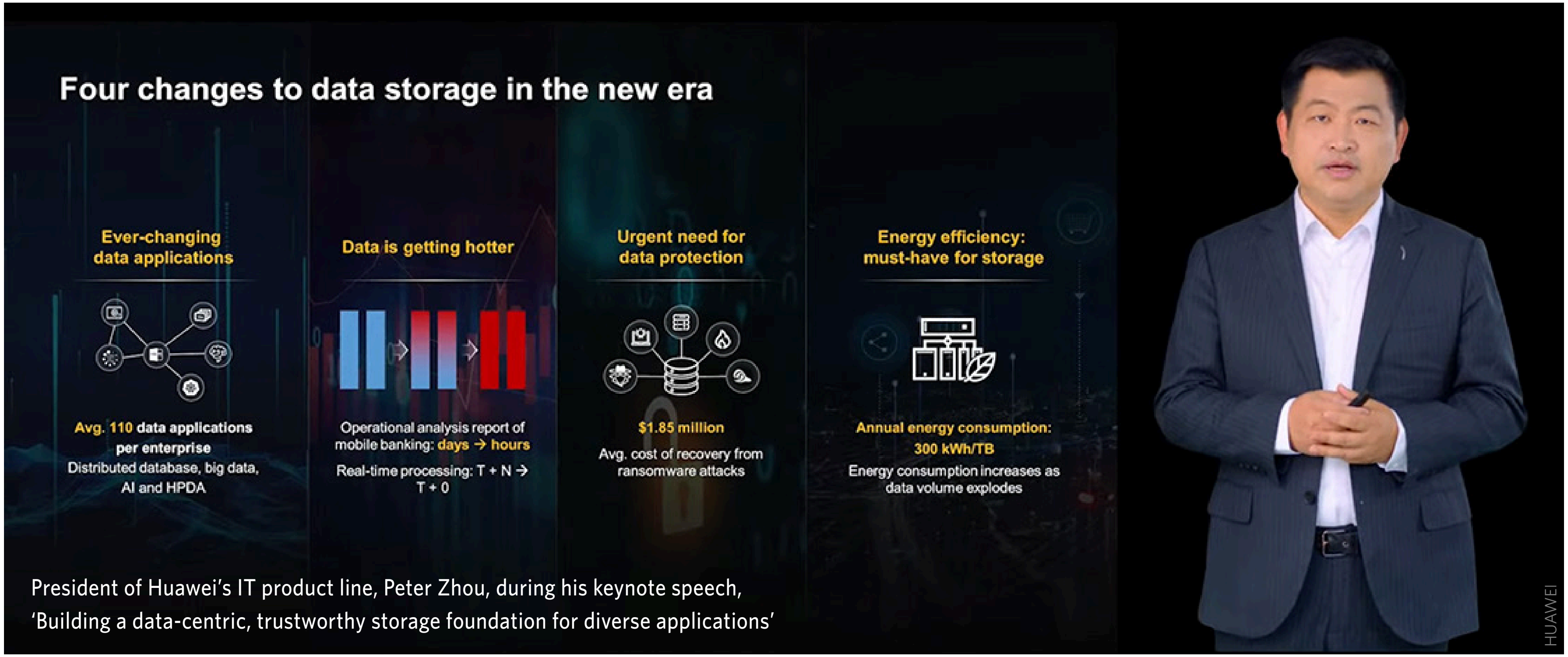
Secondly, this increasing emphasis on data will necessitate faster analytics and processing. Companies will have to operate in real time to reap the benefits of this information – there can't be any hold-ups in the system.

Then there is the issue of security to contend with. Companies are under attack more than ever. According to the Ponemon Institute's latest state of cyber security report, small and medium-sized enterprises (SMEs) worldwide are facing an increasing number of attacks, with 66% experiencing a breach, or attempted breach, in the past 12 months. Companies that are looking to make the most of their data will have to deal with that issue.

Finally, there is the issue of environmental concerns and how any products dealing with corporate workloads will need to be aware of carbon footprints.

Huawei believes its approach will tackle all these areas. The decoupling of storage and data will mean more efficient use of available storage, leading to more economic analysis of data.

But it goes further than that. The company sees a need for data acceleration engines within storage systems, so that future systems will combine a data persistence layer with the application acceleration engine, enabling corporations to handle all the emerging data-rich applications. Huawei argues that future systems should be built with metadata management and intensive data processing to improve the processing efficiency – the company believes a 10-fold increase in speed is possible.



Four changes to data storage in the new era

Ever-changing data applications

Avg. 110 data applications per enterprise

Distributed database, big data, AI and HPDA

Data is getting hotter

Operational analysis report of mobile banking: days → hours

Real-time processing: T + N → T + 0

Urgent need for data protection

$1.85 million

Avg. cost of recovery from ransomware attacks

Energy efficiency: must-have for storage

Annual energy consumption: 300 kWh/TB

Energy consumption increases as data volume explodes

President of Huawei's IT product line, Peter Zhou, during his keynote speech, 'Building a data-centric, trustworthy storage foundation for diverse applications'

HUAWEI

New approach to sustainability

But perhaps the most pressing innovation is the drive towards environmental protection and the reduction of carbon footprint. Here, Huawei's vision is in three parts: building equipment with renewable materials; basing system designs on a high degree of operational efficiency – for example, moving towards all-flash datacentres; and seeking to support enterprise services that optimise production operations for higher energy efficiency.

Datacentres contribute greatly to carbon emissions, but according to Luis Neves, CEO of GeSI, Europe's data sustainability organisation, there are signs that technology is changing and is tapping into corporate demands.

Speaking at the Huawei conference, Neves said there had been a sea-change among corporates. "A few years ago, no one was talking about sustainability; now it's at the top of the agenda and many people see ICT as a problem," he said. But this isn't necessarily the case, he added.

Neves cited the *Digital with purpose* report that GeSI had co-authored with Deloitte which showed that the right technologies could have a major impact on the way datacentres are constructed and lead to them meeting the UN Sustainable Development Goals. Companies like Huawei are rethinking their approach so that datacentres can become ever more powerful without increasing their carbon footprint. By 2025, datacentres could become 10 times more efficient, he said.

"ICT has the potential to maintain global CO_2 emissions at a low level, decoupling economic growth from emissions growth," Neves added.

In keeping with this theme at the event, Huawei talked up its moves to an all-flash environment – a key part of its aim to keep carbon emissions down and increase organisations' ability to harness data effectively. The use of all-flash can consume 70% less power and can reduce the required physical footprint by 50%, it said.

> "A few years ago, no one was talking about sustainability; now it's at the top of the agenda and many people see ICT as a problem"
> Luis Neves, GeSI

Many more companies are now looking to develop all-flash installations. According to IDC research, flash-based systems accounted for more than 40% of the global market – and when hybrid flash systems are thrown into the mix, the figure rises to nearly 80%. It wasn't all that long ago that flash was seen as a luxury; now it is seen as a must-have.

And that fits in very nicely with Huawei's agenda. While the company is probably best known in the UK for its mobile telecoms ventures, it is quietly moving forward in what is proving to be a fast-growing area and the company hopes it has the products and services that will meet the expected levels of demand. ■

EDGE STORAGE

Edge storage: What is it, and what technologies does it use?

VISUAL GENERATION/ADOBE

Storage is moving from the datacentre to the edge. Stephen Pritchard defines edge storage and looks at the characteristics of edge computing

HOME

Large, monolithic datacentres at the heart of firms could give way to hundreds or thousands of smaller data stores and devices, each with their own storage capacity.

The driver for this is organisations moving their processes to the business "edge". Edge computing is no longer simply about putting some local storage into a remote or branch office (Robo). Rather, it is being driven by the internet of things (IoT), smart devices and sensors, and technologies such as autonomous cars. All of these technologies increasingly need their own local edge data storage.

Industry analysts Gartner confirm business data is moving from the datacentre to the cloud and the edge. The firm identifies four use cases for edge storage: distributed clouds and datacentres, data processing at the edge, content collaboration and access, and digital ingest and streaming.

This isn't an exhaustive list – applications such as autonomous vehicles that sit outside enterprise IT are driving edge computing, too. Meanwhile, industrial processes, sensors and IoT are all drivers that push more computing to the edge.

The market for edge storage is being shaped by changes in storage technology and applications. Increasingly, edge devices need persistent storage that is robust and secure, but applications also demand performance that goes beyond the SD or micro-SD cards found in early-generation IoT devices and single-board computers.

Where is the edge?

A few years ago, edge computing was most closely associated with remote or branch office deployments. For storage, Robo was about providing at least some level of backup or replication to secure data, especially if a device failed, and caching or staging data before sending it to the datacentre for further processing.

This batch-based approach worked well enough in retail and other environments with fairly predictable data flows. But adding storage by way of a networked PC, a small server or a network-attached storage (NAS) device only really works in office or back-office environments, because they are static, environmentally stable and usually reasonably secure.

Today's business edge is much larger and covers much more hostile operating environments. These range from the factory floor, with edge devices attached to manufacturing equipment and power tools, to cameras and other sensors out in the environment, to telecoms kit and even vehicles.

ALTHOUGH ENCRYPTION PROTECTS AGAINST DATA LOSS, IT WILL NOT PREVENT SOMEONE PHYSICALLY REMOVING THE MEMORY MODULE

Enrico Signoretti, an analyst at GigaOM, describes these environments as the industrial edge, remote edge or far edge. Storage needs to be reliable, easy to manage and – given the number of devices firms might deploy – a cost-effective solution.

Characteristics of an edge storage system

Edge applications require storage to be physically robust, secure physically and virtually – often encrypted – and able to withstand temperature fluctuations and vibration. It needs to be persistent, but draw little power. In some cases, it also needs to be fast, especially where firms want to apply artificial intelligence (AI) to systems at the edge.

Alex McDonald, Europe, Middle East and Africa (EMEA) chair at the Storage Networking Industry Association (SNIA), says edge storage includes "storage and memory product technologies that provide residences for edge-generated data including SSDs [solid-state drives], SSD arrays, embedded DRAM [dynamic random-access memory], flash and persistent memory".

Range of environments

In some cases, storage and compute systems need to be adapted to operate in a much wider range of environments than conventional IT. This requires physical robustness and security measures. Single-board computers, for example, often rely on removable memory cards. Although encryption protects against data loss, it will not prevent someone physically removing the memory module. "Ruggedised and enhanced specification devices will support environments that require additional safeguarding in embedded applications, from automotive to manufacturing," says McDonald.

Organisations working with edge computing are also looking at storage-class memory (SCM) and non-volatile memory express over fabrics (NVMe-oF), as well as hyper-converged infrastructure (HCI). Hyper-converged infrastructure, with its on-board storage, is perhaps best suited to applications that may need to scale up in the future. IT teams can add HCI nodes relatively easily – even in remote locations – without adding significant management overheads.

But for the most part, edge computing's storage requirements are relatively small. The focus is not on multiple terabytes of storage, but on systems that can handle time-sensitive, "perishable" data that is then analysed locally and passed on to a central system – usually the cloud – or a combination of both.

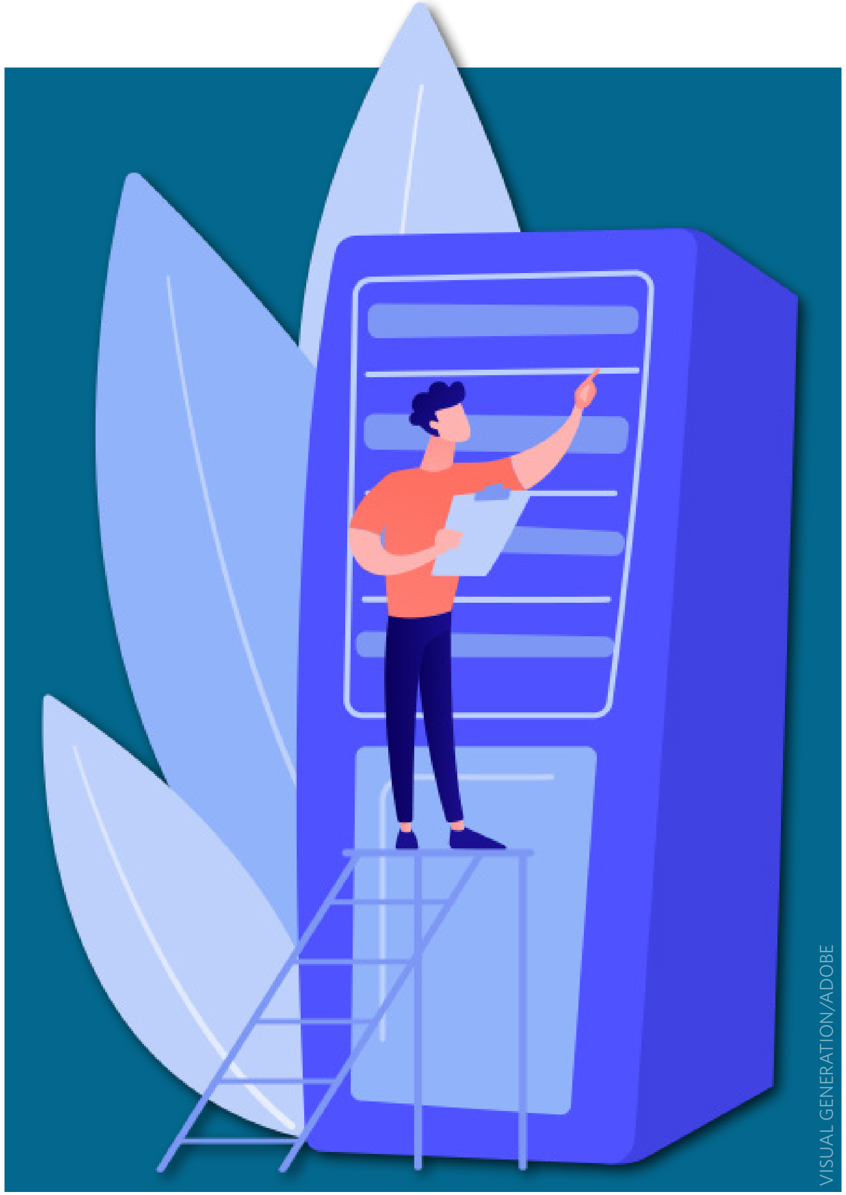
This requires systems to be able to perform immediate actions on the data, such as analytics, before passing it on to a central store or process. This data triage needs to be nimble and, ideally, close to the compute resources. This, in turn, has prompted interest in NVMe-over-fibre channel and storage-class memory.

And, by putting some local storage into the device, system designers can minimise one of edge computing's biggest challenges: its demands on bandwidth.

Edge computing's data problem

Organisations that want to add data storage to their edge systems do so, at least in part, to reduce demands on their networks and centralised datacentres, or to reduce latency in their processing.

Some firms now have so many edge devices that they risk overwhelming local networks. Although the idea of decentralised computing connected to the cloud is attractive, in practice, network latency, the possibility of network disruption and even



VISUAL GENERATION/ADOBE

cloud storage costs have prompted device manufacturers to include at least support for local storage.

Gathering data

A growing number of suppliers also make edge appliances that work alongside (or more accurately, just behind) IoT devices to gather data from them. Some are data transfer devices, such as [Google's Edge Appliance](), while some take on some of the AI processing itself, offloading it from the network.

By doing this, systems architects can provide a more robust form of edge computing. More data is processed near to the sensor or device, decisions can be made more quickly via analytics or AI, and the amount of data sent to the corporate local area network or cloud service can be vastly reduced.

Adding storage to the edge, directly or via appliances, also allows for replication or batch-based archiving and makes it easier to operate with intermittent or unreliable connections, especially for mobile applications.

Jimmy Tam, CEO of Peer Software, says that some suppliers are integrating hard disk drives in combination with SSDs to allow devices to store larger data volumes at a lower cost. "In the case where the edge storage is mainly focused as a data ingestion platform that then replicates or transmits the data to the cloud, a larger proportion of storage may be HDD [hard disk drive] instead of SSD to allow for more data density," he says.

Emerging storage technologies for the edge

It seems unlikely that any single storage technology will dominate at the edge. As Gartner noted in a recent research report: "Although edge storage solutions possess common fundamental principles, it is not a single technology, because it needs to be tailored to the specific use cases."

> GARTNER EXPECTS TO SEE MORE DATA STORAGE TECHNOLOGY BEING 'EDGE READY', INCLUDING DATACENTRE TECHNOLOGIES THAT WORK BETTER WITH THE DEMANDS OF THE EDGE

Nonetheless, Gartner expects to see more data storage technology being "edge-ready", including datacentre technologies that work better with the demands of the edge.

IoT and other edge suppliers will work to improve storage performance, especially by moving to server and workstation-class storage, such as Flash, NVMe and NVMe-oF, as well as storage-class memory, rather than USB-based technologies such as SD or micro-SD.

But the real focus looks set to be on how to manage ever-larger numbers of storage-equipped devices. Developments such as 5G will only increase the applications for edge computing, so firms will look for storage that is not just rugged, but self-healing, and, at least in normal operations, can largely manage itself. ■

GUALTER FATIA/GETTY

Siu in court

Cristiano Ronaldo has chased his pearl-clutching condemnation of Manchester United's unbridled marketing drive with the announcement of his own NFT collection.

The preening Ozymandias of football is only the latest example of unregulated crypto's insidious invasion, something *The Athletic's* Joey D'Urso attributes to it being "the cheapest way of reaching young men, who form the bulk of buyers".

The likes of Cristiano's friend, Jordan Peterson, may well weep at the idea of the Pessi generation requiring any form of introspection ever – those are also his punters, after all – but that doesn't make it untrue. Our only hope now is that this macho, neoliberal cyber hellscape can be detoxified by the honest magic of the FIFA World Cup Qatar 2022™. ■

> "The FCA has not been given regulatory oversight over direct investments in cryptoassets and NFTs. There are no consumer protections for those who buy them. If you buy cryptoassets, you should be prepared to lose all the money you invest"
>
> The Financial Conduct Authority

› Read more on the Downtime blog.