



# DIGITALISATION WORLD

MODERN ENTERPRISE IT - FROM THE EDGE TO THE CORE TO THE CLOUD

ISSUE IX 2023

DIGITALISATIONWORLD.COM

A full-page background image of a dense forest with tall, thin trees and a misty atmosphere. The ground is covered in fallen leaves and some green undergrowth.

**Becoming Forest Positive:**  
Don't just go beyond, regenerate

AI Ops | Apps + DevOps | Artificial Intelligence | Big Data + Analytics | Cloud + MS  
DC Facilities + Colo Digital Business | IT Management + Service | Networks + Telecoms  
Open Source | Security + Compliance | Storage + Servers



# Realize your company's IT potential

Software to design, monitor, and manage your IT space

62% of IT outages can be attributed to IT infrastructure failure<sup>1</sup>. Our Data Center Infrastructure Management (DCIM) 3.0 offer provides device monitoring, health assessments, and more so you can:

- Run simulated impacts to expose vulnerabilities in IT infrastructure and address them immediately
- Reduce physical threats by monitoring IT environmental conditions
- Improve sustainability efforts by tracking PUE, energy, and carbon emissions

#CertaintyInAConnectedWorld

[apc.com/edge](https://apc.com/edge)



EcoStruxure™ IT  
modernized DCIM

APC Smart-UPS™  
Modular Ultra

<sup>1</sup>Uptime Institute Global Data Center Survey, 2018

# VIEWPOINT

By Phil Alsop, Editor

## IT repeats itself

YES, it's not just history where the apparently obvious lessons of the past are spectacularly ignored in the present, so the same mistakes can be made over and over and over again – sadly with very real consequences for individuals, nations and indeed the whole planet.

In fairness, the IT industry's repeating is more in the nature of a change in attitude, often brought about by an accompanying change in technology. So, for a while, centralised everything is the only game in town, and then there are some compelling reasons why moving everything close to the end user is the only possible way forward. And then we move back to centralisation, then distributed. Although we then, somewhat sensibly (at least compared to those who ignore history's lessons) come up with a compromise – hybrid everything is good. So, some local, some regional, some centralised.

Indeed, care to name any IT technology or trend, and there seems to be a growing consensus after however many in/out iterations, that hybrid is best. Air cooling for IT kit in data centres is the only game in town; liquid cooling has to be everywhere to deal with modern, dense workloads; finally, a mixture of air and liquid, depending on the application, is the optimal solution. And so it is with cloud – public, private and finally to hybrid cloud.

So, I am being somewhat unfair when I try and draw parallels between history-ignoring politicians and the IT industry's movers and shakers, who tend to get to the right place in the end, however long the journey might take.

I was prompted to write this comment as a result of the news story in these pages which suggests that customers are 'fed up' with multi-vendor environments and like the idea of a single vendor solution. And I know from recent discussions with Channel-focused




organisations that there seems to be a growing view that MSPs in particular want to rationalise the number of vendors with which they deal. Dare I say it, the end solution seems to be rather obvious – a hybrid approach, whereby certain technology solutions might be supplied by a single vendor, but when it comes to cybersecurity, for example, the best solution will require input from several vendors.

Okay, so an end user might want to rely on one channel partner to deliver everything, but that presupposes that this one organisation will have the best of breed technology solutions across a whole range of IT disciplines – highly unlikely.

In conclusion, if history does repeat itself, but lessons really are learnt, then all for the good. Happily, that seems to be the case for the IT sector. As for the politicians, well I edit Digitalisation World, so I will leave the editors of the various history publications to decide on the cyclical nature of world events and whether any lessons are ever learnt!







## Becoming Forest Positive: Don't just go beyond, regenerate

26

As the world's desire for sustainability grows to help combat climate change, businesses are proactively looking to explore ways to embed sustainable and regenerative practices

### 14 Gartner identifies the Top 10 strategic technology trends for 2024

Gartner has published its list of 10 top strategic technology trends that organizations need to explore in 2024

### 18 Cloud Concentration now a significant emerging risk

The risk associated with dependence on a particular cloud provider for multiple business capabilities is in the top five emerging risks for organizations for the second consecutive quarter, according to a survey by Gartner, Inc

### 22 AI will reshape the IT industry

International Data Corporation (IDC) has published its worldwide information technology (IT) industry predictions for 2024 and beyond. This IDC FutureScape report provides IDC's top 10 predictions on the future of the IT Industry and how "AI Everywhere" will affect technology decisions as organizations seek to extend their digital business efforts

### 28 Why ZTNA needs to be updated to meet modern working demands

Zero Trust has become the standard security approach for many organisations. Based on the principle of not trusting any user, device, or application by default, the security framework has seen rapid adoption

### 30 Securing the distributed enterprise

Is Zero Trust the answer? Asks Aron Brand, CTO and member of the founding team of CTERA

### 32 Software for a sustainable lifecycle

In recent times, data centres have become the focus of much attention, as demand rises, energy costs soar, and sustainability issues persist

### 34 Is your office struggling to support today's collaboration demands?

Over the past three years, online collaboration tools have become the norm. Working life is largely underpinned by wireless connected laptops in place of connected docking stations and wired connections to the corporate network.



## 36 How IT teams are using AIOps to unlock growth

By moving from reactive to proactive management, companies can fuel transformative results for their IT operations and the wider business, offering customers and employees the seamless experience they demand

## 38 What we mean when we talk about the power of Hybrid Cloud (and how to get there)

Today 'hybrid cloud' has become a generic term that gets used to mean a million things to a million people. Here, I want to avoid generalisations and go deep into why the hybrid cloud has become the default IT focus for most mature organisations

## 40 Everything will be connected

Even though 5G networks are expected to grow and develop for years to come, technology strategists are already offering up visions that look far beyond 5G. If their 6G scenarios become reality, we can expect a wonderland of communications in the 2030s

## 46 Protecting digital trust from erosion

Every successful IT attack against companies makes consumers doubt whether they want to continue using their data and these services



48

## NEWS

### 06 AI to dominate 2024

### 07 CIOs and CTOs struggle with multiple vendor model

### 08 Toxic 'Tech Bros': 1 in 5 men believe women are less suited to tech roles

### 09 Digital world class technology organisations deliver more value

### 10 Zero Trust now the norm for most companies

### 11 CISOs' biggest worry is inaccurate data on security posture

### 12 One third of global enterprises have hired an employee they've never met in person



10

## 48 How to cure cloud connectivity headaches with software-defined cloud interconnect

The evolution of cloud technology has left business decision-makers spoilt for choice when searching for the cloud providers that best support their needs

## 50 Disaster recovery is not the same as ransomware planning

Cyber threats continue to rise at an exponential rate in today's digital age. Ransomware attacks are constantly in the news – seemingly on a daily basis

## DW DIGITALISATION WORLD

**Editor**  
Philip Alsop  
+44 (0)7786 084559  
philip.alsop@angelbc.com

**Sales & Marketing Manager**  
Shehzad Munshi  
+44 (0)1923690215  
shehzad.munshi@angelbc.com

**Senior B2B Event & Media Executive**  
Mark Hinds  
+44 (0)2476 718971  
mark.hinds@angelbc.com

**Marketing & Logistics Executive**  
Eve O'Sullivan  
+44 (0)2476 823 123  
eve.osullivan@angelbc.com

**Director of Logistics**  
Sharon Cowley  
+44 (0)1923 690200  
sharon.cowley@angelbc.com

**Design & Production Manager**  
Mitch Gaynor  
+44 (0)1923 690214  
mitch.gaynor@angelbc.com

**Publisher**  
Jackie Cannon  
+44 (0)1923 690215  
jackie.cannon@angelbc.com  
**Circulation & Subscriptions**  
+44 (0)1923 690214  
circ@angelbc.com

**Directors**  
Scott Adams: CTO  
Sukhi Bhadal: CEO



Digitalisation World is published 10 times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication. Angel Business Communications Ltd.  
© Copyright 2023. All rights reserved. Contents may not be reproduced in whole or part without the written consent of the publishers. The paper used within this magazine is produced by chain of custody certified manufacturers, guaranteeing sustainable sourcing. ISSN 2396-9016 (Online)

**Published by:** Angel Business Communications Ltd, 6 Bow Court, Burnsall Road, Coventry CV5 6SP  
T: +44 (0)2476 718970 E: info@angelbc.com



# AI to dominate 2024

Extended reality (XR), cloud computing, 5G and electric vehicles also among the top five most important technologies in 2024.

IEEE, the world's largest technical professional organisation dedicated to advancing technology for humanity, has released the results of "The Impact of Technology in 2024 and Beyond: an IEEE Global Study," a new survey of global technology leaders from the U.S., U.K., China, India and Brazil. The study, which included 350 chief technology officers, chief information officers and IT directors, covers the most important technologies in 2024 and future technology trends. To learn more about the study and the impact of technology in 2024, visit <https://transmitter.ieee.org/impact-of-technology-2024/>

Telecommunications, manufacturing, financial industries most impacted by technology in 2024

The top five industry sectors that will be most impacted by technology in 2024, according to survey responses, are:

- (41 percent) telecommunications (as compared to 40 percent in 2023)
- (39 percent) manufacturing (as compared to 30 percent in 2023)
- (39 percent) banking and financial services (as compared to 33 percent in 2023)
- (31 percent) automotive and transportation (as compared to 39 percent in 2023)
- (31 percent) energy (as compared to 33 percent in 2023)

AI will be the most important technology in 2024 – used in diverse ways, across the global economy. What areas of technology will be the most important in 2024? From over a dozen areas of technology, when asked to select the top three, respondents chose:

- (65 percent) Artificial Intelligence (AI), including predictive and generative AI, machine learning (ML) and natural language processing (NLP)
- (28 percent) Extended reality (XR), including metaverse, augmented reality (AR), virtual reality (VR) and mixed reality (MR)
- (24 percent) cloud computing

Other important technologies in 2024 include 5G (22 percent), and electric vehicles (20 percent). In 2024, AI applications and algorithms that can optimise data, perform complex tasks and make decisions with human-like accuracy will be used in diverse ways, the study finds. Of top potential applications for AI next year, technology leaders surveyed selected:

- (54 percent) real-time cybersecurity vulnerability identification and attack prevention;
- (42 percent) increasing supply chain and warehouse automation efficiencies
- (38 percent) aiding and accelerating software development, automating customer service
- (35 percent) automating customer service
- (34 percent) speeding up candidate screening, recruiting and hiring time
- (32 percent) accelerating disease mapping and drug discovery
- (31 percent) automating and stabilising utility power sources

Survey participants were asked what percentage of jobs across the global economy in 2024 will be augmented by AI-driven software, and 26-50 percent of jobs was cited by 41 percent of those surveyed. Over one-quarter (28 percent) cited 1-25 percent of jobs; another 26 percent cited 51-75 percent of jobs, and 5 percent cited 76-100 percent of jobs.

## Benefits of Extended Reality (XR), Digital Twin Technologies, 5G and 6G

According to the IEEE survey, virtual simulations using extended reality (XR) and digital twin technologies to more efficiently design, develop and safely test product prototypes and manufacturing processes will be important in 2024 (63 percent very important, 29 percent somewhat important).

Respondents see 5G benefitting the following areas the most in

2024, including greater benefit to transportation infrastructure and sustainability as compared to 2023.

- (54 percent in both 2024 and 2023) telemedicine, including remote surgery, health record transmissions
- (46 percent in 2024 vs. 49 percent in 2023) personal and professional day-to-day communications
- (46 percent in 2024 vs. 56 percent in 2023) remote learning and education
- (43 percent in 2024 vs. 51 percent in 2023) entertainment, sports and live event streaming
- (39 percent in 2024 vs. 29 percent in 2023) transportation and traffic control
- (27 percent in 2024 vs 25 percent in 2023) manufacturing/assembly
- (30 percent in 2024 vs 23 percent in 2023) carbon footprint reduction and energy efficiency

Close to nine out of 10 of global technologists (88 percent) agree 6G will primarily be an evolving work in progress in 2024, but will be standardised in the next 3-5 years.

In addition, a strong majority (94 percent) of global technologists agree that development of communication satellites for mobile connectivity will bring parity to some rural and developed regions globally in 2024.

## Don't count Quantum out

Generative AI may continue to dominate the technology landscape, but other technologies such as quantum will have significant, if less-noticed impacts (87 percent agree, including 51 percent who strongly agree). Furthermore, 86 percent of respondents agree, in 2024 quantum computing will gain the most attention for significantly higher computing power – a trillion times higher than that of today's most advanced supercomputers, as well as for its application to post-quantum cryptography and cybersecurity.



# CIOs and CTOs struggle with multiple vendor model

IT leaders seek to consolidate support and services into a single vendor to achieve greater agility, control vulnerabilities, and improve cost efficiency.

RIMINI STREET has published findings of the Censuswide Buyers Sentiment Survey, "IT Leaders are Considering a New Support and Services Model," examining the challenges of ERP and database support, vendor relationship management, and the need for a better IT support and services model.

The research was conducted among a sample of more than 600 U.S. respondents, consisting of CIOs and CTOs in companies with over \$250m in revenue. It is the second in a two-part series of reports from Censuswide, following the recent "Organizations Want More Control Over Their IT Roadmap" report. The survey results show that organizations are juggling an increased number of vendors, products, and services in the enterprise applications portfolio, putting stress on today's support models and straining the IT budget. Nearly three quarters of respondents say these models are inadequate in supporting their IT and business needs.

"Over the past decade, enterprises have deployed a growing number of enterprise software systems and supporting technologies to run their business. This has left them dependent on a tangled web of software vendors and service providers to support and manage these mission-critical systems," said David Rowe, EVP, Global Transformation and chief product officer. "The data illustrates that this system simply isn't working for the enterprise customer.

Without a concerted effort across the providers, it places greater responsibility on IT leaders to coordinate and manage the various systems and vendors. Today, there's a better alternative: Consolidating support and services into a single strategic partner that prioritizes business success and works closely to help plan and execute a digital

transformation roadmap that fits the company's goals."

CIOs and CTOs Say Multi-Vendor Support and Services Model Lacks Agility and Accountability  
Key findings include:

- When asked to assess the support and services they receive for their Enterprise Resource Planning (ERP) systems, databases, and related technology, 72% of CIOs and CTOs say the vendor-based model is inadequate, citing a lack of accountability (62%) and lack of expertise (46%) as top challenges
- With challenges of managing multiple support and service providers, respondents cited the different process per vendor (36%), the high cost of several vendor contracts (35%), and too much effort selecting and managing vendors (35%) as the greatest pain points
- 61% of respondents want to consolidate support and managed services into a single provider

The data shows that technology leaders are experiencing critical challenges with their IT support and services. A lack of accountability means that companies may suffer recurring product issues as there is often no root cause resolution, forcing them to explain the same problem to their individual vendors over and over again. In addition, the vendor support teams frequently offer limited expertise, leading enterprises to consult independent experts or escalate to their own experienced engineers. This costs organizations critical time and resources.

## Vendor Consolidation is Just the First Step in Addressing Complexity

The report specifically details how relying on support and services from multiple vendors makes operations even more complex and expensive for CIOs and CTOs. In these multi-



vendor models, respondents state that different vendors blame each other for problems (34%), service handoffs are lost between vendors (29%), and project lead times are longer (27%).

These problems extend beyond just cost and operational complexity, also harming cybersecurity efforts. The multi-vendor support and services model can have a multiplying effect on existing security issues. The data reveals these five top security challenges:

- Keeping up with the volume of vulnerabilities on a quarterly basis (31%)
- Balancing operational resources between "keeping the lights on" and strategic priorities (30%)
- Finding a way to stay ahead of an increasing volume of threats (30%)
- Avoiding business disruptions by security enhancements (30%)
- Upgrading software to be eligible for security patches (29%)

Offering a single point of support and service to today's technology leaders is just the first step in addressing the challenge of the multiple vendor-based support and services model. Providers must also ensure they can demonstrate the added value that consolidation brings, such as the ability to give objective, agnostic, and personalized roadmap guidance.

Ultimately, IT leaders are looking to their providers for agility, flexibility, and for a strategic partner to help plan their digital transformation roadmap and see it through to success.



# Toxic 'Tech Bros': 1 in 5 men believe women are less suited to tech roles

New research from the Fawcett Society and Virgin Media O2 has revealed that a fifth of men working in tech roles believe that women are naturally less suited to working in the sector.

TODAY'S NEW REPORT, 'System Update: Addressing the Gender Gap in Tech', is the culmination of eight months of extensive research, interviews and polling. It explores the experience of women who work in tech roles, those who have recently left and women who have the qualifications but are not working in the sector to understand the barriers and disincentives. It exposes a widespread toxic 'tech bro' culture, with 72% of women in tech roles having experienced at least one form of sexism at work. This includes being paid less than male colleagues and sexist 'banter' (22%) and questioning of their skills and abilities (20%).

On top of this, Black and minoritised women have experienced additional levels of exclusion, with almost three in four having experienced racism at work. The issue is particularly acute for Black women, with one in three having been assumed not to hold a technical role. Instead, women were assumed to work in marketing or HR, or to be present in a meeting only to take the minutes. This culture is affecting the recruitment and retention of women in the industry, creating an even greater gap in a sector suffering from talent shortages and in turn damaging our economy.

## Recruitment

Almost a third (32%) of women working in tech roles believe there is a gender bias during recruitment, with 14% having been made to feel uncomfortable because of their gender during the application process.

Women with STEM qualifications are highly suited to a career in technology, and indeed more than a third of them (36%) who aren't currently working in the sector are interested, rising significantly for Black and minoritised women (59%). However, many are put



off by their perceptions of the industry and who it's for. More than a quarter of women outside of tech think there is more sexist behaviour in tech than other types of work, 29% believe there is a lack of flexible work and more than a third (36%) think there is a lack of part-time work available.

## Retention

As a result of these factors, the research found that of those who do enter the workforce, more than 4 in 10 (43%) consider leaving their role at least weekly. Of those who have left, one in five women said it's because of caring responsibilities, and 22% of Black and minoritised women say it's because of an exclusionary culture. Nisha Marwaha, Director of People Relations and DE&I at Virgin Media O2, said: "The findings in this report are clear: The 'Tech Bro' culture is causing long term damage and creating an environment where women wrongly don't feel they belong.

"With a fifth of men harbouring an ill-conceived belief that women aren't up to the job, we must do better as businesses at creating an inclusive and diverse environment that shatters these stereotypes. Otherwise, at a time when the tech sector is hit with skill shortages, we'll miss out on a wealth of top talent."

"At Virgin Media O2, we know that diversity is the key to a brighter, more innovative, and prosperous future for all. That's why we've proudly partnered

with the Fawcett Society to champion the cause of gender diversity in tech and are committed to reviewing every recommendation in detail to accelerate change."

Jemima Olchawski, Fawcett Society Chief Executive said: "This report rings alarm bells for a sector that prides itself on being future-facing. It's unacceptable that so many women are being locked out of tech because damaging and plain wrong sexist ideas are thriving in a predominantly male workforce. It's really no surprise that 4 in 10 women consider leaving their role when toxic 'tech bro' cultures are so widespread, and women are diminished by male colleagues. And, yet again, our research shows things are even worse for Black and minoritised women who experience the compounded effects of sexism and racism.

"It makes no sense that in the midst of a skills shortage so many capable and talented women are either locked out of the sector or choosing to leave. All of this means tech firms are missing out on a wealth of talent and both women and our economy are being held back. We need urgent action to bring in a system update and create workplaces that truly respect and accommodate women in all our diversity."

To help enhance gender and racial diversity and combat biases to make the tech industry a more inclusive place for women, Fawcett Society is calling for businesses, government and schools to work together to achieve change by: Reducing bias at application: Ensuring job advertisements promote all reasonable flexible work options by default; banning salary history questions; using gender-neutral language; and setting targets to improve the representation of women and underrepresented groups.



# Digital world class technology organisations deliver more value

Digital world class technology organisations deliver far greater value than their peers, are more resilient and better able to navigate uncertainty, while also spending 18% less and operating with 27% fewer staff, according to new research from The Hackett Group.

THE HACKETT GROUP® found that while typical companies have seen technology operating costs as a percentage of end-user equivalent increase by 23% over the past 10 years, a select group of - what Hackett calls “digital world class organisations” - have seen only a 16% cost increase. The research showed that their overall reduced IT costs generate a \$37 million annual advantage (for a typical \$10 billion company).

They are also able to modernise their technology landscape through digital transformation, implementing intelligent automation, advanced analytics, cloud enablement and collaborative tools, which enable them to spend 45% less than typical companies on IT outsourcing and further reduce labour costs. Overall, their discipline and ability to maintain strategic focus allows them to adapt more rapidly to changing circumstances. By harnessing data more effectively, they can make better decisions and focus on areas that matter most, such as managing costs, without sacrificing long-term IT strategy and goals.

The Hackett Group defines “digital world class organisations” as those that achieve top-quartile performance in business value (a composite of stakeholder experience, digital enablement and traditional effectiveness metrics) and operational excellence (a composite of efficiency and business process automation metrics) in its comprehensive technology benchmark. The research is based on an analysis of results from recent benchmarks, performance studies, and advisory and transformation engagements at hundreds of global companies.

A public version of the study, “Resilience: The Digital World

Class Technology Advantage,” is available free, with registration, at <https://go.poweredbyhackett.com/rdwcatech2306sm>. It contains nearly 40 metrics detailing the performance gap between digitally advanced technology organisations and their peers – plus six key areas where these companies excel and a proposed action plan to close the gap.

Hackett’s research revealed an undeniable correlation between digitally world class status and improved overall enterprise performance. The data concluded that companies with at least one business services function operating at these levels see a five-year average performance premium over their industry medians, including: an 80% improvement in net margin; 24% higher earnings before interest, taxes, depreciation and amortisation margin; 89% greater return on equity; and 44% higher total shareholder return.

Beyond the cost and staffing advantages, the organisations excel across a wide range of business value and operational excellence metrics.

Among the highlights:

- 2.9% more projects that deliver targeted return on investment
- 47% more perceived as a valued business partner and 29% more perceived as proactive by stakeholders
- 68% higher allocation of technology spend to emerging technologies
- 62% fewer applications per end user
- 66% more IT business intelligence reports distributed automatically or via self-service

The also spend very differently than their peers, investing 68% more in emerging technologies such as artificial intelligence (AI), workflow automation and more to drive operational

effectiveness and productivity gains. This puts them in a better position to address the fact that growing workloads in the business functions are outpacing budgets and headcounts.

IT’s role expands in business transformations that require implementing new technologies, streamlined processes and introducing innovative solutions, including generative AI, to drive efficiency and improve business outcomes.

Many companies’ digital transformation efforts are already using generative AI to streamline operations, enhance customer experiences and drive business growth. IT organisations have also begun using generative AI to drive improvements in enterprise application development, deployment and management. IT leaders should also be fully involved in any adoption of generative AI technology across the revenue, operations and selling, general and administrative (SG&A) functions, to ensure that appropriate technology selection, training, security and ethics issues are addressed.

The Hackett Group Global IT Executive Advisory Program Practice Leader, Tammy Pinter, explained that, “While typical technology organisations may want to focus on value, they often don’t know where the value is in their organisation. At the same time, digital world class ones are laser-focused on driving strategic advantage.

They prioritise carefully, standardise processes consistently and focus on end-to-end process design and ownership to eliminate inefficiency. This enables them to invest in key areas that can deliver the greatest return on investment. And they have rigorous governance in place to help make it happen.”



# Zero Trust now the norm for most companies

Globally 62% of organisations (61% in EMEA) have a Zero Trust strategy in place, up from 24% in 2021.

ZERO TRUST (ZT) has become the default cybersecurity strategy for global business, according to the 2023 State of Zero Trust Report, released today by identity leader Okta.

For the first time since Okta started issuing the State of Zero Trust Report in 2019, the number of organisations that already have a defined Zero Trust strategy in place, far exceeds those still in planning stages (or without such a strategy).

“We now live in a Zero Trust world,” said Stephen McDermid, EMEA CSO for Okta. “The global figures suggest that within 18 months, nine in every 10 businesses will ‘be ZT’. And businesses are putting their cybersecurity money where their Zero Trust mouth is. Despite widespread cost-cutting, 60% of organisations have seen an increase of up to 24% in their ZT budgets since last year.”



In 2021, fewer than one in four of the organisations surveyed had a ZT strategy in place. By 2023, this number has grown to 61%. In addition, a further 28% plan to implement Zero Trust within the next year and a half.

The report suggests that leaders recognise the primary importance of Zero Trust in enabling today's digital business. The research shows 93% of the global C-Suite now believe that Identity is important to their business strategy.

## The strategy in practice: are passwordless technologies set to explode?

The report demonstrates that, despite growing knowledge of the low assurance value, passwords remain the standard for authentication - and are in use at more than half (55%) of our respondent's organisations, across all regions.

Security questions were the second most commonly used practice, with just 19% (less than 1 in 5) of businesses) using high-assurance factors like platform-based authenticators and biometrics.

“In a world where businesses must never trust and always verify, the method of verification is critical,” continued McDermid. “The uncomfortable truth behind recent attacks is that verification based on passwords and simple questions is not enough. Social engineering has evolved dramatically and as such, so should the front line of identity verification. In practice, this will mean passwordless technologies.”

## The “People” Factor: security trumps usability – for now

As an insight into the drivers behind this need to address social engineering, respondents to the research cited “People” as the biggest security concern for businesses with “Network” and “Data” coming in a distant second and third, respectively. While the user has always been rated a top priority, this year it's an unusual outlier, reflecting an increasing understanding of the critical function of identity, in Zero Trust security initiatives.

In the face of this perception that the user remains the weakest link, more than two in three companies either say security is the unquestioned top priority or that their current priority balance is three-quarters security, one-quarter usability.

However, the research also reveals that holes still remain. Only 1 in 5 (20%) of respondents have automated provisioning/deprovisioning for external users such as partners and contractors. This suggests that companies remain especially vulnerable to attacks from within the supply chain.

McDermid added: “Companies have long since recognised that either through malice or simple poor practice, their people represent the single biggest security threat, but these figures suggest that businesses may have been too narrow in the definition of ‘their people’. Suppliers and partners are – from a security perspective – just as risky as an employee. But there seems to be a lag in addressing this.”

## Is regulation creating early innovators?

Within this incredibly active global market, there are some clear leaders when it comes to embracing ZT. Companies in financial services and software are more likely to have an initiative in place today (at 71% and 68%, respectively).

58% of public sector organisations have a ZT strategy, with almost another third planning to implement one in the next 12 months.

“It is easy to see the impact of regulation on these figures,” concluded McDermid. “Some industries will face tighter demands that necessitate Zero Trust and drive the market in the short term. We welcome this catalyst for innovation and look forward to seeing what early adopters can show the wider industry.

“The past two years have seen a huge jump in the number of businesses that say identity is a critical part of their Zero Trust strategy. Now that Zero Trust is set to define how business is done, it follows that getting identity right will be a major factor in making that business easier, faster, and better.”

# CISOs' biggest worry is inaccurate data on security posture

Security leaders more worried about data quality than budget shortfall or being blamed for breaches.

PANASEER has published its 2024 Security Leaders Peer Report. Now in its fourth year, the research provides insights into the conundrum many CISOs are facing surrounding the purpose and value of security controls data in supporting critical business decisions.

The survey of senior cybersecurity decision makers in 1,000+ employee organizations in the UK and US found that the biggest concern when taking on a new CISO role is receiving an inaccurate audit of the company's security posture (54%). This is a tacit acknowledgment that inaccurate security data can hide points of weakness and result in security resources not being utilized efficiently. The issue of data quality was of greater concern to respondents than the lack of security budget (44%) and being scapegoated for a breach (44%).

The same desire to gain complete visibility into security controls data was also highlighted in the top challenges cited by respondents when starting a new CISO role:

- Getting a true picture of weaknesses in organizational security posture (49%).
- Understanding the threat landscape (45%)
- Getting trusted data to enable strategic decisions (43%)

Understanding where security controls are failing is a critical first step to mitigating cyber risk and making the right decisions. Unfortunately, only 36% of security leaders are totally confident in their security data and use it for all strategic decision making. This is a concerning finding, as without trusted data CISOs might struggle to influence senior business stakeholders and ensure the right people are held accountable for fixing security issues. "One of the most important things in the world is credibility. If you lose credibility,

it's the hardest thing to earn back from people," argues Shawn Bowen, SVP and CISO of World Fuel Services. "So when your data lacks credibility, that's the same problem. You need to know where your data is inaccurate and be up front about it, otherwise if someone else finds the inaccuracies they aren't going to trust you again."

## Perception and reality

The report found a concerning gulf between respondents' perception of their security controls and reality. Nearly all (95%) said they are highly or somewhat confident that security controls are working effectively all the time, and 88% declared that they trust their security data is accurate. As a result, over half (54%) of security leaders said they are very confident in their ability to use security data to prioritize actions to have the greatest impact on risk reduction. Nearly all (96%) are confident to some extent.

However, 79% of responding organizations admitted they have been surprised by a security incident that evaded their controls—indicating that data on the status of controls is either inaccurate, or not being properly interpreted to improve security posture. There is also evidence to suggest that controls data is not widely viewed as a strategic asset for cyber protection and risk mitigation. Over one-third of respondents (38%) said they are unable to evidence remediation of control failures. A similar number (37%) classify control failures as a low priority—rising to 43% in financial services companies.

## Restoring trust in the data

The vast majority (90%) of security leaders said that improving the accuracy of cybersecurity data is a priority for them in the next 12 months. Additionally, when asked to consider the impact of AI, 76% are concerned about threat actors using AI to find gaps

in their organizations' security controls. Given that they spend on average half (46%) of their time on manually collecting, formatting and presenting this data, finding a more automated way to do it should also be treated with some urgency. Continuous Controls Monitoring (CCM) can help to deliver the trust in this data that CISOs and other stakeholders need. The benefits of improving data quality and trust are clear, with 84% of security leaders believing that increasing trust in their data would help them secure more resources to protect their organization. But first there needs to be a mindset change in security leaders and the board—away from using controls data for reporting, and instead embracing it to proactively drive business decisions and stop problems before they occur.

"The industry needs to change if we are to solve the CISO security controls conundrum, and Continuous Controls Monitoring (CCM) can be the catalyst. It isn't a better reporting tool, it's a way of knowing what to do next – making day-to-day cybersecurity firefighting easier and getting ahead of the game on strategic risk," argues Panaseer Security Evangelist, Marie Wilcox.

"At the moment, many leaders don't know that security controls data can help them do this. It's understanding the value of a big picture view, and single source of truth rather than multiple siloed perspectives."

In this way, access to trusted controls data could not only help CISOs address the challenges and concerns listed above, but also tackle their three top priorities in a new role, as cited by respondents:

- Understanding security posture (39%)
- Understand processes for data collection and analysis (38%)
- Audit of security tooling (37%)



# One third of global enterprises have hired an employee they've never met in person

43% of global CIOs believe that having a flexible working policy has opened the door to a wider pool of highly skilled individuals.

RESEARCH of global CIOs from Expereo reveals that large global enterprises' ambitions for global growth are being constrained, as one third admit they struggle to hire high-value knowledge workers that will drive forward their global expansion plans. As a result, almost a third (32%) of global CIOs have had no choice but to hire someone they have never met in person.

The competition for talent is real. The research of over 650 CIOs in global enterprises across Europe, US and APAC reveals that skills and resource retention (35%) is currently amongst the top three barriers to their business delivering global growth, alongside challenging security environments (35%) and complicated physical and geo-political infrastructure (33%). More specifically, finding the right mix of business and technology skills was revealed to be the most challenging thing for 40% of CIOs to recruit for.

Almost a third (31%) of CIOs say that finding the right competencies for their team in governance and regulatory compliance is a challenge, while expertise in growth technologies such as cyber security (49%) AI/ML (41%), and data analytics (38%) tops the list as the most challenging skills to recruit for.

Fortunately, 43% of global CIOs say having a hybrid/remote policy has enabled them to hire from a wider geographical pool of talent; 38% say their team is now based in different countries/markets.

## Hybrid working needs to stay, but it isn't without challenges

The nature of work has changed, and almost half (48%) of CIOs believe flexible working is the key driver for retaining and recruiting the most skilled employees. Today's IT leaders are empowered to tap into a global pool of workers and partners to find the best talent, explaining why a third of CIOs (32%) have admitted to hiring someone into their team that they have never met in person.

According to the research, working three days in the office or less is now the new normal for almost three-quarters (72%) of businesses, with almost half (44%) of global CIOs believing the increased demand for hybrid/remote working is being driven by cost of living pressures. Having said that, a third of global CIOs expect to see an increase in the number of days they expect people to work from the office. According to 32% of respondents, this is due to productivity

concerns with employees working from home; 31% said home connectivity issues for their employees has a consistent impact on productivity.

## The connectivity trade-off

However, the trade-off of access to more and better skilled employees is that, for many CIOs, ensuring application performance across multiple locations (41%), and providing 24/7 support across multiple time zones (37%), are putting pressure on their teams.

Ben Elms, Chief Revenue Officer at Expereo comments; "As organisations focus on driving growth through global expansion, there are clearly complexities and challenges to overcome in supporting the evolving needs of a global workforce. With more people working from different locations, the ability to change the dynamics of the network to meet diverse connectivity needs at a moment's notice is vital.

"The key is having the technology in place that enables connectivity and collaboration in a remote world. In the end, hybrid working is all about staying connected, and enabling interaction with colleagues and customers - wherever you are in the world."

## WEBINARS

Specialists with 30 year+ pedigree and in-depth knowledge in overlapping sectors



For more information contact:

Jackie Cannon T: 01923 690205 E: jackie@angelwebinar.co.uk W: www.angelwebinar.co.uk  
T: +44 (0)2476 718 970 E: info@angelbc.com W: www.angelbc.com

**Expertise:** Moderators, Markets, 30 Years + Pedigree

**Reach:** Specialist vertical databases

**Branding:** Message delivery to high level influencers via various in house established magazines, websites, events and social media

Angel   
BUSINESS COMMUNICATIONS

# Introducing the ET60/ET65 Enterprise Tablets



It's a rugged **tablet**.

It's a rugged **laptop**.

It's a rugged **vehicle mount mobile computer**.

It's **everything** you need...all in one tablet.



For more information, please visit [www.zebra.com/et6x](http://www.zebra.com/et6x)



© 2023 ZIH Corp and/or its affiliates. All Rights Reserved. Zebra and the stylized Zebra head are trademarks of ZIH Corp, registered in many jurisdictions worldwide. 06/05/2023

\* Citizens Band Radio Service (CBRS) only available in the US.

Maximize productivity and business efficiency with the business tablets that deliver more — more features, more power, more security, more ruggedness and more versatility.



**Designed to handle practically everything** — survives more real-world tests than any other tablet in its class



**A display you can see everywhere** — because your workers can be anywhere



**Extraordinary lifecycle** — buy it for 4 years, with available support for 8 years



**It's 3 devices in one** — use it as a tablet, a laptop and a vehicle mount computer



**Trailblazing processor powers it all** — the latest wireless networks and apps



**The most powerful wireless connections** — 5G, Wi-Fi 6E, private 5G and CBRS\*



**Power it your way** — standard or extended removable batteries, or power vehicle mounted tablets with your forklifts



**Barcode scanning at its finest** — standard or extended range scanning to capture barcodes as far as 40 ft./12 m away



**Mobility DNA only from Zebra** — complimentary software tools make Zebra devices easier to use, support and manage

## DW ROUNDTABLE

Modern Enterprise It - From The Edge To The Core To The Cloud

Not every discussion is a  
**heated debate...**



- Based around a hot topic for your company, this 60-minute recorded, moderated ZOOM roundtable would be a platform for debate and discussion
- Moderated by an editor, Phil Alsop, this can include 3 speakers
- Questions prepared and shared in advance

**Cost: £5995**

**Contact:** Jackie Cannon  
[jackie.cannon@angelbc.com](mailto:jackie.cannon@angelbc.com)

**ANGEL  
EVENTS**





## Gartner identifies the Top 10 strategic technology trends for 2024

Gartner has published its list of 10 top strategic technology trends that organizations need to explore in 2024

“TECHNOLOGY DISRUPTIONS and socioeconomic uncertainties require willingness to act boldly and strategically enhance resilience over ad hoc responses,” said Bart Willemsen, VP Analyst at Gartner. “IT leaders are in a unique position to strategically lay down a roadmap where technology investments help their business’s sustenance of success amidst these uncertainties and pressures.” “They and other executives must evaluate the impacts and benefits of strategic technology trends, but this is no small task given the increasing rate of technological innovation,” said Chris Howard, Distinguished VP Analyst and Chief of Research at Gartner. “For example, generative and other types of AI offer new opportunities and drive several trends. But deriving business value from the durable use of AI requires a disciplined approach to widespread adoption along with attention to the risks.”

**The top strategic technology trends for 2024 are:**

### **Democratized Generative AI**

Generative AI (GenAI) is becoming democratized by the confluence of massively pretrained models,

cloud computing and open source, making these models accessible to workers worldwide. By 2026, Gartner predicts that over 80% of enterprises will have used GenAI APIs and models and/or deployed GenAI-enabled applications in production environments, up from less than 5% early 2023. GenAI applications can make vast sources of information — internal and external — accessible and available to business users. This means the rapid adoption of GenAI will significantly democratize knowledge and skills in the enterprise. Large language models enable enterprises to connect their workers with knowledge in a conversational style with rich semantic understanding.

### **AI Trust, Risk and Security Management**

The democratization of access to AI has made the need for AI Trust, Risk and Security Management (TRISM) even more urgent and clear. Without guardrails, AI models can rapidly generate compounding negative effects that spin out of control, overshadowing any positive performance and societal gains that AI enables. AI TRISM

provides tooling for ModelOps, proactive data protection, AI-specific security, model monitoring (including monitoring for data drift, model drift, and/or unintended outcomes) and risk controls for inputs and outputs to third-party models and applications. Gartner predicts that by 2026, enterprises that apply AI TRISM controls will increase the accuracy of their decision making by eliminating up to 80% of faulty and illegitimate information.

### AI-Augmented Development

AI-augmented development is the use of AI technologies, such as GenAI and machine learning, to aid software engineers in designing, coding and testing applications. AI-assisted software engineering improves developer productivity and enables development teams to address the increasing demand for software to run the business. These AI-infused development tools allow software engineers to spend less time writing code, so they can spend more time on more strategic activities such as the design and composition of compelling business applications.

### Intelligent Applications

Intelligent applications include intelligence — which Gartner defines as learned adaptation to respond appropriately and autonomously — as a capability. This intelligence can be utilized in many use cases to better augment or automate work. As a foundational capability, intelligence in applications comprises various AI-based services, such as machine learning, vector stores and connected data. Consequently, intelligent applications deliver experiences that dynamically adapt to the user. A clear need and demand for intelligent applications exists. Twenty-six percent of CEOs in the 2023 Gartner CEO and Senior Business Executive Survey cited the talent shortage as the most damaging risk for their organization. Attracting and retaining talent is CEOs' top workforce priority, while AI was named the technology that will most significantly impact their industries over the next three years.

### Augmented-Connected Workforce

The augmented-connected workforce (ACWF) is a strategy for optimizing the value derived from human workers. The need to accelerate and scale talent is driving the ACWF trend. The ACWF uses intelligent applications and workforce analytics to provide everyday context and guidance to support the workforce's experience, well-being, and ability to develop its own skills. At the same time, the ACWF drives business results and positive impact for key stakeholders.

Through 2027, 25% of CIOs will use augmented-connected workforce initiatives to reduce time to competency by 50% for key roles.

### Continuous Threat Exposure Management

Continuous threat exposure management (CTEM) is a pragmatic and systemic approach that allows organizations to evaluate the accessibility, exposure

and exploitability of an enterprise's digital and physical assets continually and consistently. Aligning CTEM assessment and remediation scopes with threat vectors or business projects, rather than an infrastructure component, surfaces not only the vulnerabilities, but also unpatchable threats. By 2026, Gartner predicts that organizations prioritizing their security investments based on a CTEM program will realize a two-thirds reduction in breaches.

### Machine Customers

Machine customers (also called «custobots») are nonhuman economic actors that can autonomously negotiate and purchase goods and services in exchange for payment. By 2028, 15 billion connected products will exist with the potential to behave as customers, with billions more to follow in the coming years. This growth trend will be the source of trillions of dollars in revenues by 2030 and eventually become more significant than the arrival of digital commerce. Strategic considerations should include opportunities to either facilitate these algorithms and devices, or even create new custobots.

### Sustainable Technology

Sustainable technology is a framework of digital solutions used to enable environmental, social and governance (ESG) outcomes that support long-term ecological balance and human rights. The use of technologies such as AI, cryptocurrency, the Internet of Things and cloud computing is driving concern about the related energy consumption and environmental impacts. This makes it more critical to ensure that the use of IT becomes more efficient, circular and sustainable. In fact, Gartner predicts that by 2027, 25% of CIOs will see their personal compensation linked to their sustainable technology impact.

### Platform Engineering

Platform engineering is the discipline of building and operating self-service internal development platforms. Each platform is a layer, created and maintained by a dedicated product team, designed to support the needs of its users by interfacing with tools and processes. The goal of platform engineering is to optimize productivity, the user experience and accelerate delivery of business value.

### Industry Cloud Platforms

By 2027, Gartner predicts more than 70% of enterprises will use industry cloud platforms (ICPs) to accelerate their business initiatives, up from less than 15% in 2023. ICPs address industry-relevant business outcomes by combining underlying SaaS, PaaS and IaaS services into a whole product offering with composable capabilities. These typically include an industry data fabric, a library of packaged business capabilities, composition tools and other platform innovations. ICPs are tailored cloud proposals specific to an industry and can further be tailored to an organization's needs.



### Gartner unveils top predictions for IT organizations and users

Gartner has revealed its top strategic predictions for 2024 and beyond. Gartner's top predictions explore how generative AI (GenAI) has changed executive leaders' way of thinking on every subject and how to create a more flexible and adaptable organization that is better prepared for the future.

"GenAI presents an opportunity to accomplish things never before possible in the scope of human existence," said Daryl Plummer, Distinguished VP Analyst at Gartner. "CIOs and executive leaders will embrace the risks of using GenAI so they can reap the unprecedented benefits.

"This is the first full year with GenAI at the heart of every strategic decision, and every other technology-driven innovation has been pushed out of the spotlight," added Leigh McMullen, Distinguished VP Analyst at Gartner. "GenAI has broken the mold and has kept building more excitement."

Gartner analysts presented the top 10 strategic predictions during Gartner IT Symposium/Xpo, taking place here through Thursday. By 2027, the productivity value of AI will be recognized as a primary economic indicator of national power.

This is the first full year with GenAI at the heart of every strategic decision, and every other technology-driven innovation has been pushed out of the spotlight

National governments have a strong commitment to AI and are prioritizing strategies and plans that recognize AI as a key technology in both private and public sectors. Incorporating AI into long-term national planning is being reinforced through the implementation of corresponding acts and regulations to bolster AI initiatives.

"Implementation at a national level will solidify AI as a catalyst for enhancing productivity to boost the digital economy," said Plummer. "Successful implementation of large-scale AI initiatives necessitates the support and collaboration of diverse stakeholders, showcasing the mobilization and convening ability of national resources." By 2027, GenAI tools will be used to explain legacy business applications and create appropriate replacements, reducing modernization costs by 70%.

"The maturity of large language models (LLMs) offers an opportunity for CIOs to find credible and

long-awaited mechanism for modernizing legacy business applications in a cost-effective manner," said Plummer. "CIOs can create dedicated testing units to test the output generated by GenAI LLMs, while establishing change management and upskilling processes to enable the workforce to maximize productivity throughout the modernization cycle."

By 2028, enterprise spend on battling malinformation will surpass \$30 billion, cannibalizing 10% of marketing and cybersecurity budgets to combat a multifront threat. The most effective malinformation influences humans' and machines' decision-making mechanisms and can be extremely hard to detect and shut down. Malinformation presents threats across three disparate functional areas: cybersecurity, marketing and AI.

"The rapid rise of GenAI has put fire under the feet of regulators about including malinformation as one of the risks associated with the increasing power and availability of GenAI to bad actors," said Plummer. "Enterprises who maintain a close watch on bad actors, regulators and providers of tools and technology that help combat malinformation are likely to gain significant advantage over competitors."

By 2027, 45% of chief information security officers (CISOs) will expand their remit beyond cybersecurity, due to increasing regulatory pressure and attack surface expansion.

Responsibilities for security management and digital assets are fragmented across multiple divisions and teams, with the CISO overseeing the overall digital asset portfolio. This creates inconsistencies in support for regulatory disclosures, assurance of digital security and effective management of security incidents, reducing the overall performance of the organization.

Expanding the portfolio of the CISO will enable a unification of security management, providing oversight of the consolidated security incident management process throughout the organization. By 2028, the rate of unionization among knowledge workers will increase by 1,000%, motivated by the adoption of GenAI.

Executives are quick to call out AI as a cause of positions being eliminated. Therefore, it is important for executive leaders to communicate clearly with their employees their intent for internal AI deployments. This will avoid the unintended consequences of AI anxiety building among staff. Organizations that adopt GenAI and fail to clearly address AI anxiety amongst their knowledge workers will experience 20% higher rates of turnover.

"Organizations should focus their AI efforts on worker augmentation to improve productivity and

quality of work, rather than role automation,” said Plummer. “Stay grounded in what the technology can and cannot deliver, because there remains a substantial amount of hype influencing board expectations.”

In 2026, 30% of workers will leverage digital charisma filters to achieve previously unattainable advances in their career.

A digital charisma filter prompts and sifts communications to make them more socially effective in various situations. They nudge in the moment of and before and after interactions to make leaders and co-workers more effective in the social circumstances where they wish to excel. Digital charisma filters will improve organizations’ abilities to expand hiring to include more diverse workers.

“Organizations can expand their talent pool by incorporating the use of digital charisma filter assistants to improve the congruency of interactions at all phases of recruiting and employment,” said Plummer. “Accelerate access to digital charisma assistants by pressing enterprise productivity and application vendors on how they are incorporating these capabilities into their roadmaps.”

By 2027, 25% of Fortune 500 companies will actively recruit neurodivergent talent across conditions like autism, ADHD and dyslexia to improve business performance.

“Organizations that hire and retain neurodivergent talent will experience increased employee engagement, productivity and innovation across the workforce,” said Plummer.

Fortune 500 companies are already investing in neurodiversity hiring programs and are seeing impacts on engagement and business outcomes. Organizations need to establish an outreach program to boost the discoverability of neurodiverse talent. Fast-track efforts by leveraging best practices from experts and lessons from leading organizations already working on neurodiversity.

“Include neurodivergent people in company leadership positions,” said Plummer. “Having openly neurodivergent leadership fosters a culture of inclusion and can be the most valuable action to take from the perspective of neurodivergent employees.”

Through 2026, 30% of large companies will have a dedicated business unit or sales channels to access fast-growing machine customer markets. Machine customers will force a reshaping of key functions such as supply chain, sales, marketing, customer service, digital commerce and customer experience. In fact, by 2025, more than 25% of sales and service centers in large organizations will be fielding calls from machine customers.



“Machine customers will need their own sales and service channels because they make transactions at high speeds and the volume of decision variables they use far exceed human capabilities,” said Plummer. “Machine customers will require different talent, skills and processes that may not exist in a human-customer focused division.”

By 2028, there will be more smart robots than frontline workers in manufacturing, retail and logistics due to labor shortages.

Most manufacturing, retail and logistics companies cannot find or retain enough people to support their day-to-day operations. This will cause supply chain organizations to struggle to find enough front-line workers over the next decade. Robots will help fill this gap. A December 2022 Gartner survey found that 96% of supply chain technology workers have either deployed or plan to deploy cyber-physical automation and 35% have already deployed robots, with 61% piloting or in the middle of their first implementation.

“Robotic technology is advancing rapidly, making robots viable for a growing number of front-line jobs from the factory floor to the warehouse to the retail store and beyond,” said Plummer.

By 2026, 50% of G20 members will experience monthly electricity rationing, turning energy-aware operations into either a competitive advantage or a major failure risk.

Aging grid infrastructures are limiting the ability to add electricity generating capacity, yet demand for electricity continues to increase. Enterprises are assessing energy price and accessibility as a competitiveness, which means stable access to electricity for customers will become a competitive advantage. Because of this, executive leaders are creating energy-aware operations through optimization and direct investment in energy generation.

“Leverage energy efficiency to establish long-term competitive advantage by structurally reducing energy consumptions,” said Plummer. “Assess enterprise investment by including current and future anticipated costs of energy.”





## Cloud concentration now a significant emerging risk

The risk associated with dependence on a particular cloud provider for multiple business capabilities is in the top five emerging risks for organizations for the second consecutive quarter, according to a survey.

BY GARTNER, INC.

IN SEPTEMBER 2023, Gartner surveyed 294 risk executives about their views on emerging risk or over-the-horizon risks. The Gartner 3Q23 Emerging Risk Report contains detailed information on the possible impact, time frame, level of attention, perceived opportunities and more for 20 emerging risks.

“The risk associated with cloud concentration is fast losing its ‘emerging’ status as it is becoming a widely recognized risk for most enterprises,” said Ran Xu, director, research in the Gartner Legal Risk & Compliance Practice. “Many organizations are now in a position where they would face severe disruption in the event of the failure of a single provider.”

Third party viability and mass generative AI availability both make the top five for a second

consecutive quarter as well, with third-party viability topping the list on both occasions.

“Third-party viability’s continued position reflects ongoing shifts in supply chain networks, uneven inflationary effects and continued labor pressures stoking fears that third-parties may become insolvent,” said Xu. “Mass generative AI availability is concerning risk leaders because almost everyone now has easy access to AI models with nascent (or nonexistent) guidelines in place.”

### Cloud Concentration

Cloud concentration risk has come about because many organizations have opted to focus their IT efforts on a handful of strategic providers in order to reduce IT complexity, and therefore also risk, cost and skill requirements. Compounding the problem, a handful of hyperscale vendors dominate global and regional markets with superior technical capabilities, business reach and partner ecosystems.

“Where organizations have chosen to go the route of hosting their IT services in public clouds, there aren’t many obvious ways to avoid concentration risk while keeping the benefits of cloud services,” said Xu. “Moreover, regulations at the country and subnational level diverge on concentration risk, anti-competition, data sovereignty and privacy rules pertaining to cloud services – further complicating the picture.”

Risk Name	Frequency (%)
Third-Party Viability	73
Evolving Sociopolitical Expectations	69
Mass Generative AI Availability	68
Cloud Concentration Risk	62
Personal Data Regulatory Fragmentation	59

Source: Gartner (October 2023) [N=294]

➤ Table 1: Top 5 Emerging Risks for 3Q23 (by Frequency)

There are three main potential consequences of this risk, according to Gartner experts.

### 1. Wide Incident “Blast Radius”

The more applications (and business processes) depend on a particular cloud provider, the greater the potential breadth of impact of a cloud service issue, which may heighten business continuity concerns.

### 2. High Vendor Dependence

Concentrated dependency on a particular vendor can reduce future technology options and allow vendors to exert significant influence over the organization’s technology future.

### 3. Regulatory Compliance Failures

Organizations may be unable to meet regulatory demands to address concentration risk across different regulatory bodies, which may have different approaches to concentration risk.

“Currently, if the benefits of public cloud use are considered strategically important to a business, there are not many obvious solutions to remove the risk altogether,” said Xu. “That’s why it is especially important that businesses have a well-considered continuity plan to put into action should they face any major cloud service issues.”

## 50% of critical applications to reside outside of centralised public cloud

Through 2027, 50% of critical enterprise applications will reside outside of centralized public cloud locations, according to Gartner, Inc. As cloud computing markets and data center infrastructure evolve, and interest in migrating workloads grows, many enterprises struggle to identify the right partners and solutions.

“Enterprises are beginning to seek placement for workloads that have not migrated to the public cloud,” said Dennis Smith, Distinguished VP Analyst at Gartner. “This represents approximately 70% of all workloads, but the growing number of vendors, technologies and overlapping markets makes it difficult to identify the optimal infrastructure choice for an organization’s unique circumstances and needs.” There are many options for enterprises seeking infrastructure services for their workloads that now reside on-premises, ranging from vendors’ server virtualization offerings to a full suite of services provided by public cloud providers. To determine appropriate placement strategies, Gartner recommends that infrastructure and operations (I&O) leaders follow three steps.

### Evaluate Infrastructure Requirements

Many enterprises are seeking cloud-inspired solutions for existing on-premises workloads, such as business-critical applications and general-purpose workloads. These environments may be virtualized but have limited automation and self-service capabilities due to their custom-made

There are many options for enterprises seeking infrastructure services for their workloads that now reside on-premises, ranging from vendors’ server virtualization offerings to a full suite of services provided by public cloud providers.

nature. Enterprises that expand their on-premises environments to be cloud-inspired must ensure deployments address public cloud requirements. Many cloud-inspired and cloud computing solutions also offer hybrid capabilities, where common infrastructure elements and application programming interfaces (APIs) can be deployed both on-premises and in the public cloud.

### Embrace Hybrid Capabilities & CIPS

The ongoing need to support workloads that are located outside public cloud regions means that mixed cloud and non-cloud infrastructure will be needed for the foreseeable future.

“Enterprises need hybrid capabilities and always will,” said Smith. “While public clouds deliver many benefits, such as innovation, agility and scalability, their utility can be limited when deployed outside the locations chosen by public cloud providers.”

The market for cloud infrastructure and platform services (CIPS) is significantly changing and has long-term consequences to the future of enterprise IT.

The CIPS market is currently evolving into four separate markets:

- **Distributed hybrid infrastructure (DHI)**, which address the limitations of a traditional on-premises infrastructure for cloud operating model benefits, providing greater consistency and availability.
- **Strategic cloud platform services (SCPS)**, which covers the full breadth of cloud services and includes modernizing legacy applications for enterprises.
- **Container management**, which covers a range of container management offerings including Kubernetes platforms, cluster fleet management and serverless offerings.
- **DevOps platforms** which includes solutions intended to aid continuous integration/continuous delivery. All of these markets reside outside server virtualization, infrastructure consumption services (ICS) and markets related to data center infrastructure (DCI).



“Enterprises will need to navigate both the differences and overlaps across CIPS markets to choose the appropriate workload placement,” said Smith. “This includes identifying the different personas, clarifying their requirements, across both the cloud-native infrastructure and application developer affinity vectors, and mapping them to the appropriate market.”

### Choose the right partners and solutions

I&O leaders need to determine their preference for a vendor with either an inside-out approach, or outside-in. The inside-out approach entails traditional data center vendors that have added cloud services, while the outside-in approach involves cloud providers that are providing on-premises services. Additionally, leaders need to decide whether to follow a cloud-only or cloud-first approach (SCPS market) or adopt cloud more moderately (DHI market)

“I&O leaders can select the correct infrastructure solution by performing a thorough analysis of use cases and identifying the core characteristics and capabilities needed,” said Smith. “This will help determine the appropriate technologies and vendors that align with requirements.”

### Worldwide IT spending to grow 8% in 2024

Worldwide IT spending is projected to total \$5.1 trillion in 2024, an increase of 8% from 2023, according to the latest forecast by Gartner, Inc. While generative AI (GenAI) has not yet had a material impact on IT spending, investment in AI more broadly is supporting overall IT spending growth.

“In 2023 and 2024, very little IT spending will be tied to GenAI,” said John-David Lovelock, Distinguished VP Analyst at Gartner. “However, organizations are continuing to invest in AI and automation to increase operational efficiency and bridge IT talent gaps. The hype around GenAI is supporting this trend, as CIOs recognize that today’s AI projects will be instrumental in developing an AI strategy and story before GenAI becomes part of

their IT budgets starting in 2025.”

Gartner analysts are discussing the trends that are impacting the IT market during Gartner IT Symposium/Xpo, taking place here through Thursday.

### Cloud price increases bolster software and IT services spending

The software and IT services segments will both see double-digit growth in 2024, largely driven by cloud spending. Global spending on public cloud services is forecast to increase 20.4% in 2024, and similarly to 2023, the source of growth will be combination of cloud vendor price increases and increased utilization.

While inflation’s effect on both consumers and businesses plagued the devices market throughout 2022 and 2023, devices spending will begin to rebound modestly in 2024, growing 4.8% (see Table 1).

Cybersecurity spending is also driving growth in the software segment. In the 2024 Gartner CIO and Technology Executive Survey, 80% of CIOs reported that they plan to increase spending on cyber/information security in 2024, the top technology category for increased investment.

“AI has created a new security scare for organizations,” said Lovelock. “Gartner is projecting double-digit growth across all segments of enterprise security spending for 2024.” CIOs’ Change Fatigue Delays New IT Spending CIOs are experiencing change fatigue, which is often manifesting as a hesitation to invest in new projects and initiatives. This is pushing a portion of 2023’s IT spending into 2024, a trend that is expected to continue into 2025.

“Faced with a new wave of pragmatism, capital restrictions or margin concerns, CIOs are delaying some IT spending,” said Lovelock. “Organizations are shifting the emphasis of IT projects towards cost control, efficiencies and automation, while curtailing IT initiatives that will take longer to deliver returns.”

2024	2022	2022	2023	2023	2024	
	Spending	Growth (%)	Spending	Growth (%)	Spending	Growth (%)
Data Center Systems	227,021	19.7	237,703	4.7	260,221	9.5
Devices	766,279	-6.3	689,288	-10.0	722,472	4.8
Software	811,314	10.7	916,240	12.9	1,042,386	13.8
IT Services	1,305,699	7.5	1,401,038	7.3	1,547,349	10.4
Communications Services	1,423,128	-1.9	1,449,286	1.8	1,497,345	3.3
Overall IT	4,533,441	2.9	4,693,556	3.5	5,069,773	8.0

Source: Gartner (October 2023)

► Table 1.  
Worldwide  
IT Spending  
Forecast  
(Millions of U.S.  
Dollars)



## AI will reshape the IT industry

**International Data Corporation (IDC)** has published its worldwide information technology (IT) industry predictions for 2024 and beyond. This IDC FutureScape report provides IDC's top 10 predictions on the future of the IT Industry and how "AI Everywhere" will affect technology decisions as organizations seek to extend their digital business efforts.

THIS YEAR'S PREDICTIONS are largely centered around the emergence of artificial intelligence (AI) as a major inflection point in the technology industry. While AI is not a new technology – companies have been investing heavily in predictive and interpretive AI for years – the announcement of the GPT-3.5 series from OpenAI in late 2022 captured the world's attention and triggered a surge of investment in generative AI. As a result, IDC expects worldwide spending on AI solutions will grow to more than \$500 billion in 2027. In turn, most organizations will experience a notable shift in the weight of technology investments toward AI implementation and adoption of AI-enhanced products/services.

"Every IT provider will incorporate AI into the core of their business, investing treasure, brain power, and time," said Rick Villars, group vice president, Worldwide Research at IDC. "For CIOs, and digitally savvy C-Suite members, this pivot promises a cornucopia of new, innovative, AI-enhanced products/services but also threatens to inundate IT teams with many 'now with AI' options that increase risks associated with uncontrolled cost increases and loss of data control."

IDC's FutureScape 2024 research focuses on the external drivers that will alter the global business ecosystem over the next 12 to 24 months and the issues technology and IT teams will face as they define, build, and govern the technologies required to thrive in a digital-first world.

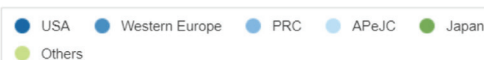
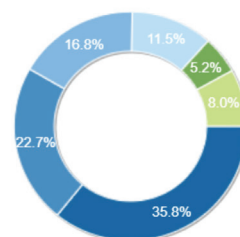
A closer look at IDC's top ten worldwide IT industry predictions reveals the following:

**1. Core IT Shift:** IDC expects the shift in IT spending toward AI will be fast and dramatic, impacting nearly every industry and application. By 2025, Global 2000 (G2000) organizations will allocate over 40% of their core IT spend to AI-related initiatives, leading to a double-digit increase in the rate of product and process innovations.

**2. IT Industry AI Pivot:** The IT industry will feel the impact of the AI watershed more than any other industry, as every company races to introduce AI-enhanced products/services and to assist their



Top Region Based on 2023 Market Share (Value (Constant))



Source: IDC Worldwide Digital Transformation Spending Guide - Use Case Forecast 2023 | Oct (V2 2023)

customers with AI implementations. For most, AI will replace cloud as the lead motivator of innovation.

**3. Infrastructure Turbulence:** The rate of AI spending for many enterprises will be constrained through 2025 due to major workload and resource shifts in corporate and cloud datacenters. Uncertainty about silicon supply will be joined by shortcomings in networking, facilities, model confidence, and AI skills.

**4. Great Data Grab:** In an AI Everywhere world, data is a crucial asset, feeding AI models and applications. Technology suppliers and service providers recognize this and will accelerate investments in additional data assets that they believe will improve their competitive position.

**5. IT Skills Mismatch:** Inadequate training in AI, cloud, data, security, and emerging tech fields will directly and negatively impact enterprise attempts to succeed in efforts that rely on such technologies. Through 2026, underfunded skilling initiatives will prevent 65% of enterprises from achieving full value from those tech investments.

**6. Services Industry Transformation:** GenAI will trigger a shift in human-delivered services for strategy, change, and training. By 2025, 40% of services engagements will include GenAI-enabled delivery, impacting everything from contract negotiations to IT Ops to risk assessment.

**7. Unified Control:** One of the most challenging tasks for IT teams in the next several years will be navigating the maturation of control platforms as they evolve from addressing a few basic systems to becoming a standard platform that orchestrates operations across infrastructure, data, AI services, and business applications/processes.

**8. Converged AI:** Today's fascination with GenAI should not delay or derail existing or other AI investments. Organizations must contemplate, trial, and bring to production fully converged AI solutions that allow them to address new uses cases and customer personas at significantly lower price points.

**9. Locational Experience:** The accelerated adoption of Gen AI will enable organizations to enhance their edge computing use cases with contextual experiences that better align business outcomes with customer expectations.

**10. Digital High Frontier:** Satellite-based Internet connectivity will deliver broadband everywhere, helping to bridge the digital divide and enabling a host of new capabilities and business models. By 2028, 80% of enterprises will integrate LEO satellite connectivity, creating a unified digital service fabric that ensures resilient ubiquitous access and guarantees data fluidity.

### Digital transformation to continue double-digit growth

Digital transformation (DX) remains a global priority as organizations seek to become digital businesses where value creation is based on the use of technologies for processes, products, services, and experiences. To achieve that objective, worldwide DX spending is forecast to reach nearly \$3.9 trillion

in 2027 with a five-year compound annual growth rate (CAGR) of 16.1%, according to the International Data Corporation (IDC) Worldwide Digital Transformation Spending Guide.

The global focus on digital transformation is reflected in the geographic distribution of DX spending. While the United States will account for 35.8% of worldwide DX spending in 2023, that figure is nearly matched by the Asia/Pacific region (including Japan and China) with a 33.5% share of spending. And the Europe, Middle East, and Africa (EMEA) region will deliver 26.8% of DX spending worldwide this year.

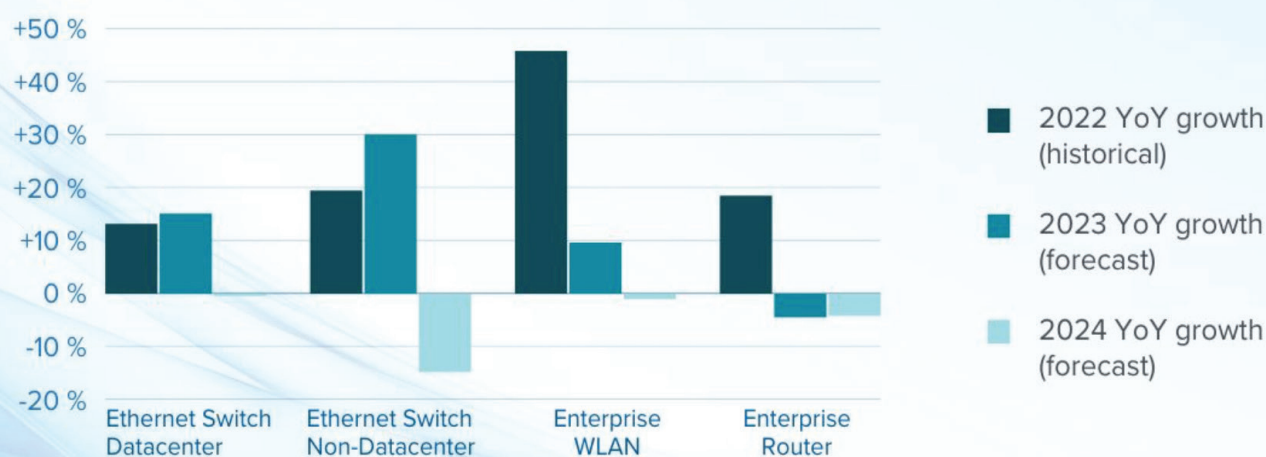
"In Europe, Digital Transformation spending is growing at a fast pace, and we estimate a CAGR of 16% across the 2023-2027 timeline. In this context, investment opportunities will vary depending on countries, industries, and use cases," said Angela Vacca, senior research manager, Data and Analytics, Europe. "The fastest growing geography will be the Nordics where Financial Services and Telecom/Media companies will be the most dynamic, growing their DX spend by more than 20% across the forecast period. In France, the fastest growing Use Case will be Machine Learning–Driven Predictive Analytics in the Healthcare Provider industry, which will grow by 32% over the period to 2027. This shows that the European market is dynamic and diverse and that opportunities need to be pinpointed."

"Digital Transformation has taken center stage across enterprises in the Asia/Pacific region as the focus continues to rapidly shift from traditional business models. Customer Experience, Innovation, and Efficiency are leading to business models that are boosting both productivity and profitability for businesses. With a young and growing population that is more tech savvy than older generations, rapid infrastructure developments towards urbanization are driving the demand for digital offerings both in products and services. Integration of multiple 3rd Platform technologies such as Cloud Computing and Artificial Intelligence coupled with a need to cater to real time customer experience will continue to push investments further across industries with specific use cases as priorities in the Asia/Pacific market," said Mario Allen Clement, associate research manager for the Asia/Pacific IT Spending Team.

The two largest DX use cases in terms of global spending are both focused on using technology to improve operational efficiency. The largest use case – Innovate, Scale, and Operate – is a broad area covering large-scale operations, including making, building, and designing activities. Core business functions that make up this area include supply chain management, engineering, design and research, operations, and manufacturing plant floor operations. The second largest use case – Back-Office Support and Infrastructure – includes core



## European Enterprise Network Vendor Revenue YoY Growth Rates



Source: Worldwide Quarterly Ethernet Switch Tracker, Worldwide Quarterly Wireless LAN Tracker, Worldwide Quarterly Router Tracker, Q22023

IDC Tracker®

business functions such as accounting/finance/billing, human resources, legal, security and risk, and enterprise IT. Combined, these two use cases will account for more than 35% of all DX spending in 2023.

Another important use case for DX investment is Customer Experience, which includes all customer-related functions and related technologies supported by DX. Core business functions that make up this area include customer services, marketing, and sales. A closely related use case is 360 Degree Customer and Client Management, which enables better engagement and experience throughout the customer journey. Together, these two use cases will represent more than 10% of all DX spending in 2023. The fastest growing among the more than 300 DX use cases identified by IDC include Mining Operations Assistance, Robotic Process Automation-Based Claims Processing, and Digital Twins with five-year CAGRs of 32.6%, 30.6%, and 28.5%, respectively.

Discrete Manufacturing is the industry with the largest DX spending throughout the forecast, accounting for roughly 18% of all investments worldwide. Some of the top use cases include Robotic Manufacturing, Autonomic Operations, Inventory Intelligence, and Smart Warehousing. The next largest industries in terms of DX spending are Professional Services, where the focus is on operational efficiency use cases, and Process Manufacturing. The Securities and Investment Services industry will experience the fastest growth in DX spending with a five-year CAGR of 21.1%, followed closely by Banking and Insurance with CAGRs of 20.0% and 19.2% respectively.

### European enterprise networking infrastructure market records strong growth

According to the latest update of the Worldwide Ethernet Switching, WLAN, and Router Trackers published by International Data Corporation (IDC), the European enterprise networking infrastructure market will grow 18.9% year on year in 2023, reaching a total value of \$14.3 billion. Demand for enterprise networking technologies, which include Ethernet switches, WLAN, and routers, will remain solid throughout the 2022-2027 forecast period, as these are key facilitators of organizations' ongoing digital transformation and play important role in AI implementation. Vendors of enterprise networking technologies posted extremely strong revenue growth in 2022, driven by an unprecedented backlog clearing. This momentum continued in the first half of 2023, leading to strong market value growth. Although the market is expected to decline by 7.6% year-on-year in 2024 due to "digestion" of delivered backlogs, the compound annual growth rate (CAGR) over the 2022-2027 period should still be positive.

"Strong revenue growth for Ethernet switching and enterprise WLAN continued in the first half of 2023, which led us to revise the 2023 forecasts significantly upwards from the previous release," says Peter Kosinar, program manager at IDC Europe. "We expect growth in these markets to decelerate in the second half of 2023, eventually turning to negative figures in 2024, mainly due to temporary market saturation after backlogs have been cleared, as well as increased IT budget constraints and the worsening macroeconomic situation in key European countries."



HEADLINE SPONSOR

**EXAGRID**

# WINNERS ANNOUNCED

THE 2023 Storage, Digitalisation and Channel (SDC) Awards Winners were announced in glamorous style at the awards evening on 30th November 2023 at the Royal Garden Hotel, London.

It was amazing to meet and greet winners at our awards ceremony. The awards presentation featured 33 proud award winners and covering categories from across the Storage, Digitalisation and Channel industries. The SDC Awards team would like to thank all those who participated this year, especially

our sponsors including; Headline Sponsors ExaGrid for their enthusiastic support our Category Sponsors HCL Group, Hornetsecurity, Infinidat, StorMagic & Schneider Electric

The SDC Awards were voted for by the readership of the Digitalisation World stable of publications and with a record number of nominations across all categories this year, the standard keeps getting higher and higher. All the Winners and Runners Up are to be congratulated on being voted 'outstanding' in their category.

Business Continuity/Disaster Recovery (BC/DR)  
Project of the Year



Storage Transformation Project of the Year




Data Security/Compliance Project of the Year

Sponsored by: **INFINIDAT**



Digital Transformation Project of the Year

Sponsored by: 



Intelligent Automation Project of the Year

Sponsored by: **INFINIDAT**



Cloud Transformation /MSP Project of the Year



Networking / Communications Project of the Year



Storage Hardware Innovation of the Year



Storage Management Innovation of the Year



Backup/Archive Innovation of the Year



Data Security/Compliance Innovation of the Year



Business Continuity/Disaster Recovery (BC/DR)  
Innovation of the Year



AI/Machine Learning Innovation of the Year



## Orchestration/Automation Innovation of the Year



## Data Management/Analytics Innovation of the Year



## IT Operations and Management Innovation of the Year

**HCLTech**

## Cloud Platform Innovation of the Year



## Cloud Storage Innovation of the Year



## Cloud Security Innovation of the Year



## Software-as-a-Service Innovation of the Year



## Infrastructure-as-a-Service Innovation of the Year



## Vendor Channel Program of the Year



## IT MSP/IT Systems VAR of the Year

Sponsored by: **EXAGRID**

**HCLTech**

## MSP/VAR Data Protection Innovation of the Year

Sponsored by: **Schneider Electric**



## Excellence in Service Award

Sponsored by: **EXAGRID**



## SDC Channel Champion Award

**datto** Greg Jones  
A Kaseya COMPANY

## Storage Company of the Year

Sponsored by: **StorMagic**



## Cloud Company of the Year



## Digital Transformation Company of the Year



## Security Vendor of the Year



## Company Culture Initiative

Sponsored by: **HCLTech**

**GIACOM.**

## Social Impact Initiative

**HCLTech**

## AI/Machine Learning Data Protection Innovation of the Year

**INFINIDAT**

## Special Recognition for Channel Security Services Award

**opentext**  
Cybersecurity



# Becoming Forest Positive: Don't just go beyond, regenerate

As the world's desire for sustainability grows to help combat climate change, businesses are proactively looking to explore ways to embed sustainable and regenerative practices.

BY NANCY POWELL UK & IRELAND SUSTAINABILITY MANAGER AT HP

FORESTS are key in helping combat climate change, but nearly half of the world's forests are under threat. The mass destruction of trees—deforestation—continues, sacrificing the long-term benefits of standing trees for short-term gain of fuel, and materials for manufacturing and construction. HP have long understood the role of Forests as both carbon sinks and important natural habitat. While replenishment has been an HP imperative for many years, we extended this to 'go beyond' with Forest Positive.

Prioritising the protection of forests is important because we're all inextricably linked to them. Last November, leaders at the COP27 climate conference in Egypt emerged with a landmark agreement aimed at protecting nature. Delegates from 26 countries formed a Forest and Climate Leaders' Partnership (FCLP), dedicated to halting and reversing forest loss – a term also referred to as 'forest positive'.



Forest positive broadly means halting and reversing nature loss - going beyond conservation and planting trees. Last year saw the term gain significant traction, as businesses now have an in-depth understanding of biodiversity trends and a role to halt climate change and biodiversity loss.

Many of the biggest companies, ourselves included, have programmes that should be increasingly scrutinised to ensure words match deeds. Here's how companies can effectively step up against deforestation and create a forest positive future.

**Lesson One: Revisiting Your Sustainability Goals**  
Sustainability in 2023 is about much more than an organisation doing the best it can for the planet. A business must have awareness, take responsibility, and be accountable for mitigating all its impacts, including those on the natural world. Above all else, being a sustainable business is about action and setting goals.

Nowadays, the majority of the world's largest companies now issue a sustainability report and set goals; more than 2,000 companies have set a science-based carbon target; and about one-third of Europe's largest public companies have pledged to reach net zero by 2050. As a rule of thumb, a business's sustainability goals should be revisited every three years to see how much progress is being made and if the goals are impactful.

Integrating forest-positive goals into your company's sustainability strategy is a key way to ensure these

goals will have a real and meaningful impact. These goals will help to protect existing forests, strengthen biodiversity, and preserve ecosystem services and can be done through tree planting initiatives or building a more sustainable product portfolio.

### **Lesson Two: Assessing the Green Credentials of your Packaging**

Increasingly, eco-conscious consumers are also opting for brands that have stringent climate action goals and can help them to reduce their carbon footprint through sustainable packaging. Sustainable packaging can be broken down into three key elements:

**Preservation:** Using non-toxic and compostable materials can help conserve the environment, reduce landfill deposits, and protect wildlife.  
**Reduction:** Reducing the amount of packaging used through redesign, such as custom-fit boxes that have a minimal void but still provide maximum protection to the contents.

**Circulatory:** Using recycled content and reusable products to close the loop on the usage of unsustainable materials. This can be achieved using packaging that can be easily and widely recycled. Metrics can be applied to assess packaging performance and determine steps that can be taken to improve its sustainability. From assessing the packaging material waste and carbon footprint it generates, to the usage of recycled and renewable content within the material.

This was a key driver in HP's quest to achieve 99% deforestation of HP brand paper and paper-based product packaging in 2020. The remaining 1% is assessed to ensure reported fibre usage meets HP's Sustainable Paper and Wood Policy.

### **Lesson 3: Partnering with Experts**

Forest conservation and restoration is a simple and effective starting point for organisations wishing to combat climate change. Trees are our allies when it comes to combatting global warming as they absorb CO<sub>2</sub> from the atmosphere which they use to grow. Like many organisations, HP's goal is to be Forest Positive by 2030 through its commitment to forest conservation. This approach involves partnerships with recognised environmental organisations, designing products and services to reduce environmental impact, and sharing tools for more responsible printing.

Since 2020, HP has worked with the Arbor Day Foundation to plant a range of native tree types in Mersey Forest that provide habitats for local species and boosts biodiversity. Restoring and protecting the world's trees and forests will be crucial in the battle against climate change and Britain's declining biodiversity. To date, HP and the Arbor Day Foundation have been responsible for planting over 40,000 trees across the UK & Ireland alone. Choosing to partner with an organisation such as

This was a key driver in HP's quest to achieve 99% deforestation of HP brand paper and paper-based product packaging in 2020. The remaining 1% is assessed to ensure reported fibre usage meets HP's Sustainable Paper and Wood Policy

the Arbor Day Foundation is one step in addressing the urgent need for reforestation. These corporate partnerships ensure initiatives add real value and prevent them from being a mere box-ticking exercise.

There are many ways for organisations to set ambitious climate action goals - from assessing the source and lifespan of their packaging materials, to tackling the need for reforestation head-on. However, each method requires careful consideration to ensure implementation is successful and drives change. Consumers have grown wise to greenwashing and actively seek out organisations that can help them to live sustainably, often being influenced by authentic brand ambassadors who align with their own beliefs.

Like any ambitious company programme, creating a truly sustainable initiative and setting clear goals designed to support a new era of opportunity can be a challenge. When momentum has slowed, unexpected obstacles emerge, and new regulations bring plans into question, it pays to remember why you are doing this: it is good for the planet, and good for business.

Partnering with knowledgeable and established third parties is key to helping companies achieve their sustainability goals. Speaking with experts to effectively deploy initiatives, such as tree planting or carbon offsetting, can be the difference between a box-ticking exercise and making a genuine contribution toward a very real issue.

I am calling on all businesses to speak with leading conservation and environmental organisations about climate change, forest restoration, and responsible management to counteract deforestation. This is an effective way for companies to reduce their environmental impact and ensure they're on track to achieve any climate goals they choose to set.





## Why ZTNA needs to be updated to meet modern working demands

In recent years, Zero Trust has become the standard security approach for many organisations. Based on the principle of not trusting any user, device, or application by default, the security framework has seen rapid adoption.

**BY MARTIN MACKAY, CRO AT VERSA NETWORKS**

OKTA'S recent report revealed that a whopping 97% of global organisations surveyed are either implementing or planning to implement Zero Trust, with over half already having done so. It's also likely that the remaining 3% are also having constructive discussions around the potential implementation of Zero Trust in the near future.

However, working environments are changing post-pandemic, and there has been a dramatic rise in hybrid work, with employees regularly working both in the office and remotely. Latest reports show that by the end of 2022, 53% of U.S. workers were engaging in a hybrid manner.

Unfortunately, current Zero Trust Network Access (ZTNA) models are yet to adapt fully to these changing tides. They remain laser-focused on remote work, often leaving on-site networks in the lurch. It's time ZTNA was brought out of the confines of remote work and adapted to meet the needs of the equally demanding realm of the office and multi-branch premises.

### Understanding the security limitations of ZTNA in a hybrid working setup

ZTNA solutions for remote workers are cloud-delivered, and they typically become inactive when the user is on-site, thereby reverting to less secure, perimeter-based security approaches in the LAN.

This disconnect between the demands of hybrid work and the current capabilities of ZTNA poses a significant challenge in terms of access security and the organisation's security posture.

Inline inspection, a crucial aspect of network security, also becomes problematic with cloud-delivered ZTNA. With inline inspection, all data passing through a certain point in the network are analysed for malicious content or behaviour. Performing this function in the cloud for on-site workers requires "hair-pinning" – going out to the cloud from the campus and back – meaning that the process is not only slow, causing significant delays, but also leads to increased costs due to the higher bandwidth and processing demands.



On-site devices, such as printers and IP phones, also become difficult to access under cloud-delivered ZTNA, posing additional operational hurdles. And OT and IoT devices that are commonly found onsite cannot accommodate the agents required by most ZTNA solutions. This is one of the primary reasons vendors turn off ZTNA when users are onsite.

Additionally, ZTNA solutions struggle to fully replace legacy security systems like Perimeter Intrusion Detection Systems (PIDS), as they do not have the ability to monitor inline network traffic onsite. These limitations accentuate the need to reimagine ZTNA to provide a holistic and efficient security protocol, suitable for hybrid work environments.

On top of these security challenges, the current design of ZTNA solutions, which have been optimised for remote settings, tend to fall short in providing the requisite application performance and policy enforcement needed by on-site workers.

### The universal Zero Trust strategy: Zero Trust everywhere

To meet the evolving demands of the modern workforce, we need to revisit and refine our understanding of Zero Trust. A holistic approach, coined 'Zero Trust Everywhere', is the key to securing both remote and on-premises users. This all-encompassing strategy looks to bridge the existing gaps in ZTNA implementation, ensuring optimal security and performance regardless of user location.

The aim of 'Zero Trust Everywhere' is extending ZTNA to all users, including remote workers and office staff, ensuring ZTNA is delivered directly in the network, thereby mitigating latency and performance issues. This strategy must cater to a range of onsite use cases, such as ZTNA for unmanaged devices, Bring Your Own Device (BYOD), contractors, and third-party access. It needs to account for both client and client-less access requirements, including ZTNA for operational technology (OT) and Internet of Things (IoT) devices, so that every component of the wider enterprise network is brought under the Zero Trust aegis. This will allow businesses to reduce their external threat landscape and ensure secure access across all components of the network.

It's also crucial that the strategy allows management of all ZTNA policies from a unified control point and repository, simplifying the task for IT teams. Moreover, 'Zero Trust Everywhere' integrates ZTNA into broader Secure Service Edge (SSE) and Secure Access Service Edge (SASE) platforms for internet/SaaS security and WAN edge optimisation. This benefits businesses and security teams by reducing the complexity of managing user access across different systems and optimising network performance, thus supporting business continuity and growth. Adopting network security solutions that embrace 'Zero Trust Everywhere' thus provides a forward-thinking and inclusive solution, catering to the needs of a diverse workforce and the wide array of devices and systems in play in today's evolving digital landscape.

## Introducing the ET60/ET65 Enterprise Tablets



It's a rugged **tablet**.  
It's a rugged **laptop**.  
It's a rugged **vehicle mount mobile computer**.  
It's **everything** you need...all in one tablet.



For more information, please visit [www.zebra.com/et6x](http://www.zebra.com/et6x)

Maximize productivity and business efficiency with the business tablets that deliver more — more features, more power, more security, more ruggedness and more versatility.



**Designed to handle practically everything** — survives more real-world tests than any other tablet in its class



**A display you can see everywhere** — because your workers can be anywhere



**Extraordinary lifecycle** — buy it for 4 years, with available support for 8 years



**It's 3 devices in one** — use it as a tablet, a laptop and a vehicle mount computer



**Trailblazing processor powers it all** — the latest wireless networks and apps



**The most powerful wireless connections** — 5G, Wi-Fi 6E, private 5G and CBRS\*



**Power it your way** — standard or extended removable batteries, or power vehicle mounted tablets with your forklifts



**Barcode scanning at its finest** — standard or extended range scanning to capture barcodes as far as 40 ft./12 m away



**Mobility DNA only from Zebra** — complimentary software tools make Zebra devices easier to use, support and manage

# Securing the distributed enterprise

Is Zero Trust the answer?

BY ARON BRAND, CTO AND MEMBER OF THE FOUNDING TEAM OF CTERA

THE DIGITAL LANDSCAPE of the modern enterprise bears almost no resemblance to the traditional corporate settings of yesteryears. With employees working from dispersed locations and applications hosted on cloud services rather than on-prem data centers, the challenge of security has evolved. In an age where you should always assume that at least one device on your network is compromised, how do you securely enable a distributed workforce to access resources in this cloud-centric world? One emerging strategy is zero trust architecture, an approach that's gaining momentum for its robust defense mechanisms.

## Understanding Zero Trust

Zero trust is founded on a simple, yet powerful, premise: never trust, always verify. This means continually authenticating and authorizing every user and device that attempts to access resources within your network. Trust is never assumed; it is continuously earned through rigorous verification protocols.

## Key concepts of Zero Trust architecture

Here are the key concepts that make this architectural framework both robust and adaptive:

**Least Privilege Access:** Under zero trust, access permissions are strictly based on need. Users are

given access only to the specific data and resources essential for their tasks, nothing more. This access is frequently reviewed and modified as user roles evolve.

**Multifactor Authentication:** This isn't your regular password-only territory. Zero trust mandates multiple forms of verification such as one-time codes, biometrics, and security keys, offering a more robust identity validation and safeguarding against compromises.

**Microsegmentation:** The network is split into small, isolated zones housing critical resources, with extremely restricted access between these zones. This minimizes the potential for lateral movement should a breach occur.

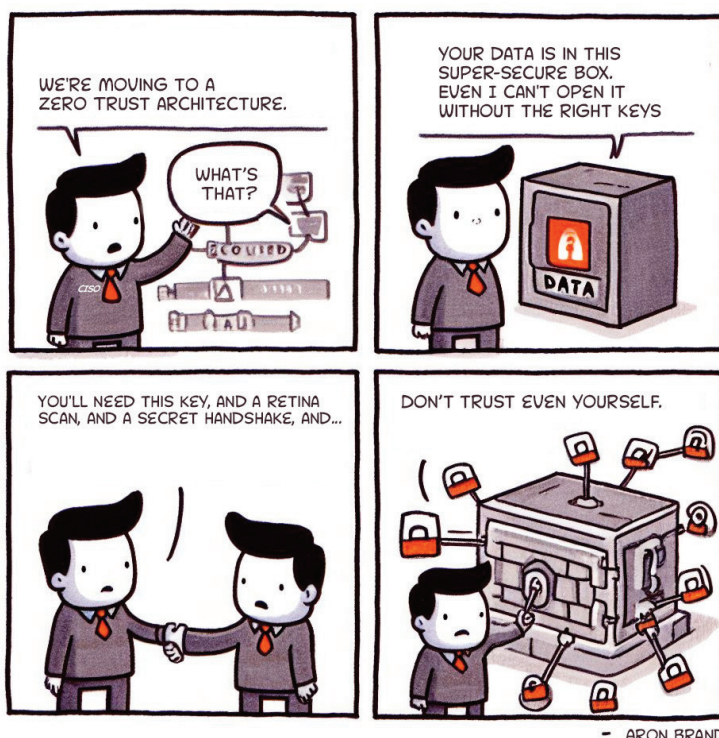
**Pervasive Encryption:** Data is encrypted both at rest and in transit using technologies like TLS, VPNs, and tokenization. Encryption serves as the last line of defense, should other security measures falter.

**Continuous Monitoring:** The network is ceaselessly scrutinized for user behavior, traffic patterns, and potential threats. This real-time oversight ensures comprehensive visibility across the distributed environment.

## Zero Trust in the age of advanced threats

In the current cybersecurity landscape, ransomware attacks stand as one of the most insidious threats, and they are far more complex than they seem at first glance. These attacks often unfold over an extended period, sometimes ranging from a day to even a month. Initially, a ransomware operator breaches a network and gains entry. They typically use tools like PSEXec to quietly collect login credentials, enabling them to spread laterally across the network.

As ransomware operators infiltrate computers within the network, they don't just lie in wait. They actively exploit the captured credentials to exfiltrate unencrypted files from backup devices and servers. Only after securing this valuable data do they proceed to deploy the ransomware, locking critical files and systems and often demanding hefty ransoms for their release. Many victims make the mistake of assuming that once the ransom is paid, the operators are gone from the system. This belief is far from the truth, as the attackers often maintain a persistent presence, posing an ongoing threat.



- ARON BRAND

This layered, complex nature of ransomware attacks underscores the need for a zero trust architecture. With its principles of least privilege access and microsegmentation, zero trust makes it exceedingly difficult for ransomware operators to propagate through a network. Even if they breach an entry point, their lateral movement is severely restricted, making it challenging to collect additional credentials or access storage devices and servers.

In addition, as generative AI technologies mature, we're seeing the emergence of AI-driven advanced persistent threats. These threats can execute complex missions, from data exfiltration to destruction, potentially combined with advanced social engineering techniques made possible by the ability of large language models to convincingly impersonate humans. Here again, zero trust proves invaluable. Its continuous monitoring and granular access controls can help in detecting and containing such concealed AI-driven threats.

Fundamentally, the guiding assumption of zero trust is that there's always a compromised device on a network. Given the complexity of ransomware attacks and the lurking presence of AI-driven threats, this assumption isn't just prudent—it's essential. Whether it's a single compromised device or a more complex network intrusion, zero trust provides a robust framework for immediate detection and containment, making it an indispensable part of modern cybersecurity strategy.

### Implementation and Compliance

Deploying a zero trust architecture isn't a trivial task; it's a strategic undertaking that demands meticulous planning and allocation of resources. Initial steps encompass mapping out all assets, network flows, and data, followed by the definition of granular access policies grounded in the principle of least privilege. Multifactor authentication is then extended across all users and devices, while encryption protocols are ubiquitously implemented. The network is subdivided into microsegments shielded by software-defined perimeters. Analytic tools are deployed to facilitate real-time monitoring. This is a 12-24 month endeavor, but it will ingrain zero trust deeply into an organization's security framework.

Zero trust also significantly eases compliance with stringent regulations like HIPAA for healthcare and PCI DSS for payment data. The architecture's inherent features such as microsegmentation and continuous monitoring are naturally aligned with the compliance requirements, reducing the compliance burden on enterprises.

### Choosing Zero Trust-embedded products for robust security

When selecting infrastructure and server applications, it's critical to opt for products that genuinely incorporate zero trust principles into their design. Far too often, vendors use zero trust as a mere marketing buzzword, lacking in-depth integration into their

products. To discern if a product is genuinely zero trust, look beyond surface-level features and evaluate its underlying architecture.

Take for example, a data storage product equipped with antivirus features, designed to synchronize data from multiple remote sites to centralized cloud storage. A simplistic antivirus implementation might scan data solely at the source computer. This runs counter to the zero trust philosophy of "never trust, always verify," because it assumes that the source computer is inherently secure. A true zero trust approach would necessitate scanning for viruses both at the source computer and again upon arrival at the cloud storage. This dual-layered scrutiny ensures that the centralized storage remains secure even if the source computer is compromised.

### Conclusion

How does one secure a distributed workforce in this complex, ever-evolving digital environment? Zero trust offers a robust framework, tailored for the challenges of the cloud age. It employs a foundational assumption of universal mistrust, augmented by multifaceted identity verification, intricate network segmentation, ubiquitous encryption, and vigilant real-time monitoring. As the cyber threat landscape continues to mutate—especially with the proliferation of ransomware and AI-driven advanced persistent threats—zero trust isn't just a contemporary remedy. It's a long-term strategy that will only escalate in strategic importance for any forward-looking enterprise.

Implementing zero trust isn't a one-time endeavor but a continuous journey—perhaps a never-ending one. It's also a careful balancing act. While the aim is to establish as secure an environment as possible, there's a counter-need to ensure that these security measures don't cripple user productivity. Stringent controls can often become hindrances, causing friction in day-to-day operations. Therefore, it's essential to strike a balance, making incremental changes while continuously monitoring their impact on both security and operational fluidity.

Moreover, when you're in the market for new infrastructure or considering an upgrade, it's crucial to think of zero trust as part of the foundational design, not just an add-on feature. Whether you're purchasing data storage solutions, networking hardware, or server applications, scrutinize how deeply zero trust principles are integrated into the product. True zero trust is not just about security features but about a holistic approach that interweaves security into every aspect of an organization's digital framework.

As you navigate the tumultuous waters of today's cybersecurity challenges, zero trust stands as a reliable compass. It's a long-haul commitment that demands both vigilance and adaptability, worthy of being a cornerstone in the security strategy of any modern, forward-thinking enterprise.





## Software for a sustainable lifecycle

In recent times, data centres have become the focus of much attention, as demand rises, energy costs soar, and sustainability issues persist.

**BY MARK YEELES, VP, SECURE POWER UK AND IRELAND, SCHNEIDER ELECTRIC**

ENERGY CONSUMPTION and efficiency have rightly come under the spotlight, but questions about capital and operational expenditure have given way to an awareness and understanding of total expenditure. Similarly, as carbon emissions are considered, so too is embodied carbon for a complete picture of lifecycle carbon assessment. Data centre resilience and sustainability can be unlocked by employing the new and emerging range of digital software and automation tools during the design stage, through operational life and even into decommissioning. Through techniques such as Computational Fluid Dynamics (CFD), digital twins, and DCIM software that can enable operators to reduce operating costs and energy consumption via automation.



Data centres can, and must, be designed, constructed, managed and operated using software and automation that ensures maximum resilience

and awareness of the impact they are having on the environment around them to future-proof their sustainability and ensure they can provide answers to global ESG goals.

### Design and build optimisation

Through the evolution of advanced software, it is now possible to digitise the infrastructure design process beyond 3D modelling and create a digital twin that can predict, through artificial intelligence (AI), the complete lifecycle of a data centre.

Tools such as energy management platforms, smart construction applications, and unified operations for data centers, can effectively create and model new facilities, allowing multiple configurations to be tried and tested before a single brick is laid. This ensures that resilience and sustainability criteria are designed and incorporated from the outset.

When combined with CFD technology, airflows can be modelled and optimised, while end-users and operators can experiment with IT layouts, capacity, and scaling to find the optimum configuration. This approach, however, can determine far more than hot aisle and cold aisle layouts.

For example, it can identify problem areas for cooling IT equipment such as hotspots, and help address them before they become an issue. Furthermore, the use of CFD software can provide insights in terms of future planning and load layout to avoid challenges with capacity utilisation. In essence, software platforms, including digital twins, have now become more sophisticated, and taking inspiration from the metaverse, are being run alongside their operational counterparts for change management, scenario exploration and experimentation. This level of digitalisation can provide greater insight, including the implementation of science-based emissions metrics, and common reporting frameworks, while addressing key points such as embodied carbon, which were previously difficult to gauge.

### Operational efficiency

Within the data centre industry too, the power of software is creating new efficiencies and opportunities to drive sustainability. Data Centre Infrastructure Management (DCIM) systems have evolved to become hosted on the cloud, thereby becoming interoperable systems architected to cope with hybrid IT, homogeneous estates and services from a multitude of data centre environments. The term DCIM 3.0 has also come into fruition, where the monitoring, management, planning, and modelling of IT physical infrastructure is made possible, with flexible deployment options that include on-premises and cloud-based solutions to support distributed IT environments from a few to thousands of sites globally.

With the assistance of AI, next-generation DCIM not only orchestrates and manages the distributed, hybrid enterprise, it brings your data to life, builds a picture of operations to offer insights for optimisation, reducing the incidence and impact of stranded capacity, and identifies underutilised or unreliable equipment in need of replacement.

### Increasing uptime

Another benefit from digitally designed facilities is that end-users and operators can become familiar with the facilities and systems digitally, before ever setting foot inside. This is seen as critical in reducing human error in maintenance and configuration changes. The 2022 Outage Analysis from the Uptime Institute, for example, reports that almost two thirds (60%) of failures now result in at least \$100,000 in total losses, with the vast majority (85%) of incidents stemming from staff failing to follow procedures or flaws in the processes themselves. An IDC estimate puts the organisational cost of human error at \$62.4 million annually.

DCIM 3.0 also facilitates predictive maintenance, further increasing resilience. As such, the software can help proactively plan maintenance cycles to reduce costs, ensure adequate levels of uptime and mitigate the potential impact of failures. Moreover, advanced software can serve as the basis for increased automation and 'lights out' operations.

### Conclusion

The new software capabilities found in digital design tools, operational systems, and modelling, can allow data centre operators to better understand the complete impact and lifecycle operation of a new facility in detail not previously thought possible. Leveraging developments in sensors, monitoring systems and advanced data analytics, modelling in the form of digital twins is giving unprecedented opportunities to meet the needs of energy efficiency, resilience and adaptability, while enabling sustainability targets to be both met and exceeded. Furthermore, the lifetime impact of a data centre can be better understood and controlled, from design and operations to decommissioning, re-use and recycling.

With digital design and development tools allied to new operational management controls, the data centres of the future will be more efficient from the day they are deployed, more resilient for their operational life, and ultimately, more sustainable.







## Is your office struggling to support today's collaboration demands?



Over the past three years, online collaboration tools have become the norm. Working life is largely underpinned by wireless connected laptops in place of connected docking stations and wired

connections to the corporate network. The hybrid worker is here to stay. But how is the office environment adapting to meet these needs, and are collaboration tools being used effectively?

**BY ROB QUICKENDEN, CTO, CISILION**

### Office environments need to quickly adapt

A survey by Microsoft Surface found that more than four in five UK workers (83%) are still in the same office environment as before the pandemic. Yet, fuelled by an increase in data centres and the growing popularity of advanced technologies such as artificial intelligence (AI), the network optimisation services market is expected to grow to \$11.84 billion in 2027 at a CAGR of 15.1%.

The make-up of the office needs to adapt quickly, and tools need to be used effectively to make hybrid working productive. There are some key areas where companies should be focusing their energy and budgets.

### Aging office networks

Pre-pandemic, a wireless network may have only been used as a guest network, but now it must support all workers requiring a wireless connection. Almost every meeting or call features video, screen and app sharing and collaborative working. To do this in real-time with good quality audio and video, businesses need the right infrastructure. For



example, some networks can't handle the increase in capacity and minimal latency that video enabled meetings and collaborative working requires.

With the acceleration of cloud adoption, combined with the birth of AI powered services such as Microsoft 365 Copilot, connectivity needs to be able to be application aware and optimise network traffic in real-time. Your Wi-Fi performance should be the first port of call when exploring a network optimisation project.

Howard Kennedy LLP, a London based, full-service law firm worked with Cisilion to refresh its core infrastructure to reflect its adoption of hybrid work across the organisation. Due to a higher demand in video conferencing and remote working, it was deemed that its existing infrastructure was no longer fit for purpose for this new way of collaborating. With its ageing Wi-Fi infrastructure approaching end of life, the solution was to optimise its corporate network for low-latency wireless connectivity. Refreshing the existing infrastructure meant switching to Cisco's Catalyst 9k family of products, providing Wi-Fi 6.

Collaboration is a requisite for the law firm, and Teams and Zoom enable this perfectly, yet the network needed to withstand 'everyone on Teams or Zoom all the time'. Wi-Fi 6 ensures that the law firm now experiences hardly any glitches on video calls in the office due to its error correction capabilities. Howard Kennedy benefits from the same network speeds as a wired connection, withstanding the increased demands for connectivity.

### Wired IP telephony is outdated

The higher demand for video conferencing now means that conference rooms with wired IP telephony are now outdated. Video conferencing software such as Microsoft Teams and Webex are now second nature.

On-premises telephony systems that are hosted in company datacentres are now being replaced by cloud-based telephony platforms that can easily integrate with Microsoft Teams and Webex. Not only does this enable improved collaboration, but it also circumvents employees needing to use call forwarding functions to their mobiles.

### Network upgrades needn't be disruptive

In most cases, new equipment can be situated in existing wired access points which can minimise disruption. In the case of Howard Kennedy, the installation of its new wireless network was completed over a weekend, causing minimal downtime. A site survey may be necessary to map out the Wi-Fi signal if the office is set across different floors to avoid dead zones. It may be necessary to add additional Wi-Fi points, however, overall a network optimisation project should be straightforward.

### Adapting the physical office space

Many organisations are transforming their traditional offices into intelligent spaces that are more appealing to work from, are more sustainable and promote a collaborative and inclusive environment that is aware and can adapt to how and where people work. These new "employee hubs" use the network to monitor air quality, people flow, and room occupancy whilst delivering secure, end-to-end cloud-managed connectivity supporting the needs of every employee.

Changes to layout and the creation of more free-flowing workspaces may be required to suit a larger number of hybrid workers. For example, the higher volume of video conferencing calls means that workers will need space to retreat from the main hub of the office. Therefore, a greater number of smaller meeting rooms or break-out areas may be more appropriate rather than a boardroom and larger conference rooms.

### Using meeting technology effectively

There have been huge advances in meeting room technology, but if adoption isn't high and people aren't taught how to use it effectively it's a waste of money. You can have the best network, great collaboration tools and amazing new energy efficient office spaces equipped with the latest video technology, but without due process for people they amount to nothing. You need to ensure your people know how to use the right tools and how to get the best from them. This is not simply about training; it's about embedding a mindset of learning too.

### The right cyber security

Security isn't about a product or a new tool. It's about ensuring your whole organisation adopts a Zero Trust approach to security rather than simply protecting the legacy network boundary that existed before. This approach ensures that employees have suitable security enabled on their devices, like two-factor authentication. Employees also need consistent training on the latest cybersecurity threats.

The right network and tools, and the right office layout and employee training, combined with great security make for successful collaboration. The result is a more empowered, engaged workforce that is highly productive.

Changes to layout and the creation of more free-flowing workspaces may be required to suit a larger number of hybrid workers. For example, the higher volume of video conferencing calls means that workers will need space to retreat from the main hub of the office



## How IT teams are using AIOps to unlock growth

By moving from reactive to proactive management, companies can fuel transformative results for their IT operations and the wider business, offering customers and employees the seamless experience they demand.

**BY MARTIN SUMMERS, APPLICATIONS, DATA AND AI PRACTICE LEADER, KYNDRYL UK & IRELAND**

IN THE CLOSING MONTHS of 2022, you couldn't go five minutes without seeing, hearing, or reading about generative AI. Heralded as the technology trend of 2023 before the year had even begun, the technology entered one of the biggest hype cycles ever seen in the tech industry. The buzz continues almost a year on, with business and government interest in AI solutions for IT far from subsiding. In fact, even companies with flat or shrinking IT budgets are looking to engage, with 63% planning to increase IT automation investments in the next year.

The vast majority (92%) of large enterprises are already using IT automation, with usage split right down the middle between a hybrid of public and on-premises systems (50%) and solely on-premises or

public cloud. The question is, how will AI unlock new opportunities for growth and wider business impact?

### The AI advantage

When it comes to a business' IT operations, agility and responsiveness should be at the top of the checklist. Whether it be switching up ways of working, expanding into new markets, or improving customer experiences, IT operations should always meet the needs of changing environments, ongoing digital transformation, and an evolving security landscape.

By increasing investment in IT automation, businesses are working towards meeting these changing needs and staying ahead of the competition. AIOps uses analytics, and machine

learning to collect the huge amounts of data that IT infrastructure generates and identify patterns that might point to performance and maintenance issues, often before users even notice.

### Resolution, and standardisation

AIOps enables businesses to “fix it before it breaks” – pinpointing and predicting what and where incidents will happen to form a proactive response. By bringing application performance and resource management together in real time, and feeding performance metrics into predictive algorithms, AIOps can map patterns and trends against different IT issues to allow for this level of proactivity.

AIOps can then automatically route alerts and recommend solutions to the appropriate teams, or even use results from machine learning to trigger an automatic response, fixing errors before users are even aware that something has happened. AI models therefore help the system and wider IT team to learn about and adapt to any changes that occur in the environment, whether that be malicious threats or simply new infrastructure deployed.

In addition, AIOps is helping businesses establish and align on guardrails across traditional and hybrid cloud environments. Microsoft, VMware, SAP and other providers are constantly publishing new best practices for their systems, hardware, and software. And compliance recommendations from organisations like the Center for Internet Security (CIS) only complicate the quest to keep up with the latest industry changes. AIOps’ policy-based automation and orchestration helps businesses manage and align on the relevant policies across multiple systems and devices, helping to safeguard the business and remove time-consuming tasks from human specialists.

### Driving business value

There are many ways in which AIOps is boosting business value for those organisations that are implementing it. The ability to rectify issues quickly – often instantly in fact – without the same level of human involvement sees improved mean time to detection (MTTD) and mean time to resolution (MTTR), ultimately reducing downtime and cutting through the noise of IT operations.

AIOps also boosts collaboration between DevOps, ITOps, governance, and security functions, allowing businesses to improve their decision making and efficiency across teams. Given the importance of IT cost optimisation in today’s financial landscape, AIOps helps to lower operational costs by automating responses and

In addition, AIOps is helping businesses establish and align on guardrails across traditional and hybrid cloud environments

freeing up staffing resources. Overall, using AI within IT offers a huge boost to both the employee and customer experience. By bolstering an IT service that resolves issues quickly, reduces organisational silos, and offers greater system visibility, the business can offer an experience that has greater lasting value for those that interact with it.

### Partnering for success

Despite interest in AIOps peaking, even for those that are actively reducing their IT budgets, only 20% of companies currently identify themselves as ‘mature’ when it comes to automation. But these mature organisations share a common facilitator – third-party partnerships. 70% indicated that they could not achieve a mature status without collaborating with the right automation partner. When seeking out a partner for AIOps, consider how their capabilities match up with your own automation solutions and goals. Look for a partner that will support you from end to end, starting with implementation, continuing with maintenance, and offering managed services post-deployment. And finally, ensure your chosen partner can scale its services as your business grows. By moving from reactive to proactive management, companies can fuel transformative results for their IT operations and the wider business, offering customers and employees the seamless experience they demand.







## What we mean when we talk about the power of Hybrid Cloud (and how to get there)

Today ‘hybrid cloud’ has become a generic term that gets used to mean a million things to a million people. Here, I want to avoid generalisations and go deep into why the hybrid cloud has become the default IT focus for most mature organisations. I’ll provide some practical examples of why it has become the default IT architecture and a great example of how best to use it. In that way maybe we can edge forward to understanding the power of deploying modern IT workloads rather than just using hybrid as a throwaway word or conference meme.

**BY VIJAY RAMAN, VICE PRESIDENT OF PRODUCTS AND TECHNOLOGY,  
CLOUD SOFTWARE GROUP**



TODAY, the number-one technical challenge for CIOs and CTOs is reaching the ability to deploy and shift workloads at any time. In the real world though, too many are still stuck with the anchor of legacy systems that weigh down attempts to move at speed and support the organisation optimally.

Getting to a hybrid cloud world where it’s fast and convenient to move between private and public clouds means lower costs, reduced risks and having a bedrock for ongoing digital transformation where you can take advantage of new cloud-native technologies as they come along.

Cloud is a great fit for business because it suits the need for the adaptivity and velocity required in a world that, for largely macroeconomic reasons, has rapidly become dangerous and unpredictable.

Cloud means IT only pays for what it uses, low-level administration, support across devices, on-tap scalability and superior cost controls, including the chance to make chargeback workable. It’s often more secure, more reliable, faster and offers inherent business continuity support. In other words, it rids IT of many of the shackles CIOs have wrestled with for decades.

But there are clouds and there are clouds. Managed clouds match the ethos of cloud advantages because they take away the need for IT to provide day-to-day support for operations. Cloud service providers help organisations they serve by providing a single-tenant solution that's tailored to individual needs for performance, security, regulatory compliance and data protection. That liberates IT leaders to do things that add real value, such as providing the data analytics capability through which executives can deliver strategies that deliver genuine competitive differentiation.

### How containers change everything

Hybrid cloud is everywhere and a major enabler of this ubiquity is the rise in importance of containers, and Kubernetes especially. Gartner research released in May 2023 predicts that 15 per cent of on-premise workloads will run in containers by 2026, compared to just five per cent in 2022. And in 2022, Datadog found that nearly half of respondents to its survey use Kubernetes.

Containers allow the granularity and composability that we all seek today to bring flexibility into our IT systems and the wider business. Contrast the effect of microservices with the old monolithic applications and the practical differences become clear. In the old world, our scope for rapid change was gated by the fact that core applications were large, complex and full of internal and external dependencies. Move one element and you could never be sure if the application as a whole would stay up or retain performance.

Containers on the other hand support portability from on-premises platforms to public or private clouds. They also represent an excellent fit for 'cloud-bursting': that is, adding an overdrive to manage spikes in demand via the addition of small workloads that are virtualised, isolated and secure. Kubernetes, in particular, has won favour because it enables the management and orchestration of containers. So, for example, clusters can be added to infrastructure to earn a performance upgrade or to bolster resilience.

Finally, containers and Kubernetes are great platforms for whatever comes next, such as cloud-native architectures, serverless and Platform as a Service.

### An Example: How Brampton blossoms with data-driven decision-making

It was the great General Electric CEO Jack Welch who said that "an organisation's ability to learn, and translate that learning into action rapidly, is the ultimate competitive advantage". Today, we use data and analytics to achieve that competitive advantage and to make smart, auditable decisions backed up by facts. So, when the Canadian city of Brampton, Ontario wanted to serve its citizens with better programmes and services, it set about creating a comprehensive data management platform that

delivers many of the benefits outlined above in terms of flexibility in IT and broader operations. Brampton, known as the "Flower Town" of Canada after its famous nurseries and greenhouses, wanted to supply its government workers with all the tools they needed to make data-driven decisions and make its services easily accessible to its 650,000 residents. To gain access to a fully-integrated data fabric, Brampton selected the ibi™ WebFOCUS business intelligence and analytics suite.

Later, in a pioneering move, it elected to move all components to the cloud for ease of access, value, and mobile device support from anywhere. Brampton uses managed cloud on Microsoft Azure with ibi™ WebFocus and Omni-Gen for data integration, plus DataMigrator and iWay Service Manager on-premises. This flexible hybrid cloud approach means the city can enjoy software, hosting and support from a single accountable source. It also means it can combine the power of data analytics with supported complementary Azure features such as elastic compute capacity.

Having this unified platform leaves staff free to focus on how best to serve Brampton's citizens with law and order, transport, recreation, emergency, parking, licensing and other services. As an example of how reliable data and visual dashboards can impact organisations outside better-managed public travel and leisure site booking, Brampton can track bylaw infractions in real time to support rapid decision-making on appropriate responses, such as creating a public information campaign to warn of risks.

### What to think about

Getting to an optimised cloud hybrid world such as that enjoyed by Brampton isn't easy for mature organisations that will often have critical workloads that are hard to move. Over time, the trend has been away from 'lift and shift' towards a pragmatic approach that sees application modernisation come to the fore. You're not alone in dealing with this pain but moving to a cloud-native world will repay efforts.

Do think carefully about who is managing your cloud and who is providing the cloud platform. Lock-in to a single cloud platform provider is a real concern so seek out providers that cover multiple cloud platforms. There are good reasons why some workloads work better on AWS, Microsoft Azure or Google Cloud, and the ability to move from one to another is highly valuable.

Finally, consider how you deploy and empower your people. Freed from the drudgery of traditional IT management, it's crucial that you provide the budget and set up to think creatively about where IT can make a difference.

This then is the real meaning of hybrid cloud: an environment where it's finally possible to do what IT was always intended to do for organisations. The rest is up to you.



# Everything will be connected

Even though 5G networks are expected to grow and develop for years to come, technology strategists are already offering up visions that look far beyond 5G. If their 6G scenarios become reality, we can expect a wonderland of communications in the 2030s.

**BY ALEXANDER PABST, VICE PRESIDENT MARKET SEGMENT WIRELESS COMMUNICATIONS AT ROHDE & SCHWARZ**



THE LTE STANDARD (4G) meets the needs of most mobile network users. Download speeds of up to several hundred megabits per second make it easy to stream high-resolution video content or download large files within seconds. 5G is available in much of the world but mostly piggybacking on LTE (NSA). Pure 5G standalone (SA) rollout will happen over the next years, yet research into the next generation of mobile communications has already started; 6G is expected to be rolled out by 2030.

But are any needs left unsatisfied by the technically advanced 5G system, which is subject to ongoing development and extension? A pair of authors posed this very question back in September 2018 [1]. What started as a discussion among experts has since gained serious momentum. Political and industrial interest in 6G has triggered a global

technological race with billions flowing into research and development.

### What needs can 6G meet?

“6G will satisfy the expectations that 5G has created,” was how Dr. Ivan Ndip from the Fraunhofer Institute for Reliability and Microintegration (IZM) pithily described the situation in an interview in spring 2021. Although 5G has yet to reach its full potential, applications are emerging that require 6G for large-scale implementation. Autonomous driving is one example.

At autonomy level 5, which is still a long way off, vehicles will not be as autonomous as the name suggests. After all, vehicles share roads, traffic lights and other infrastructure with countless other road users. For everything to run smoothly,



autonomous vehicles must be connected in three ways: with each other, with roadside facilities and with a traffic control centre. Since many situations are safety-critical, such as emergency braking, high transmission speeds and reliable signal transfer are vital

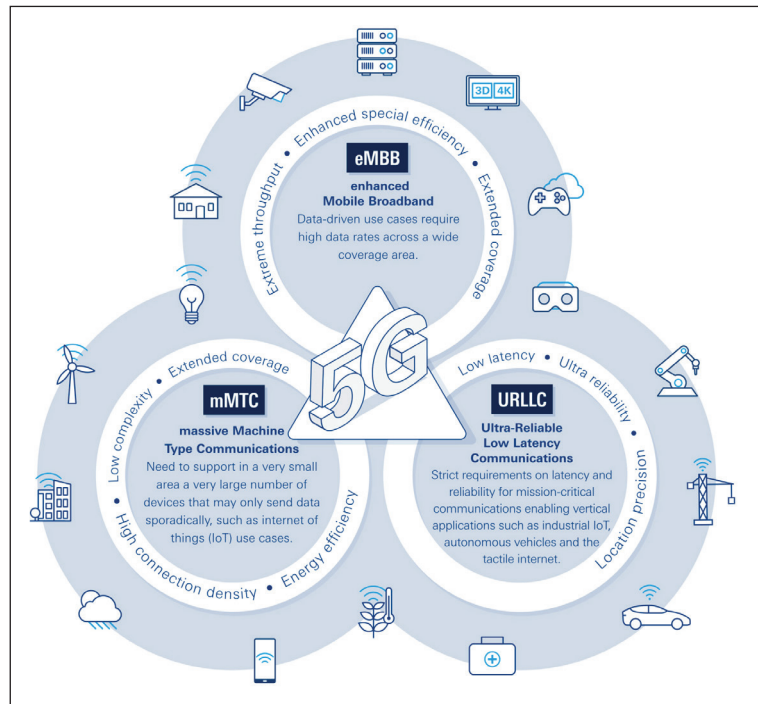
Vehicles require extremely high data rates to exchange sensor data and download detailed traffic plans. 5G is clearly a big step forward, but with a maximum data rate of 20 gigabits per second and signal latency of a millisecond, it is probably not good enough for true autonomous driving. Completely autonomous vehicles will only be possible with 6G, which is to reduce signal latency by a factor of ten and increase data throughput by a factor of fifty (Table 1).

Enhanced mobile broadband (eMBB) allows classic mobile applications but with much better performance than LTE. Massive machine type communications (mMTC) support energy efficient low-performance applications such as sensor networks. Ultra-reliable, low latency communications (URLLC) focus on real-time applications that require ensured signal transit times and availability. Autonomous driving is a key cutting-edge application that is pushing 6G research. Other important applications are extended reality (XR) and industrial automation. These sectors hinge on the ultra-low latency promised by 6G for instantaneous decision-making and seamless user experiences.

### Focus shifts to machines

In 6G, functions and services for efficient machine-to-machine communications (M2M) will play a vital role.

URLLC and mMTC (see Figure. 1) are two of three key 5G focal points in this area. In addition to autonomous driving, 5G applications include Industry 4.0, smart cities and smart homes. Rather than a single type of M2M communication, many different types are needed. Just look at a connected



factory where end-to-end signal transit times in the lower millisecond range need to be combined with minimum latency variation and highest reliability. Smart cities or smart homes have completely different requirements. A smart home needs utility meters, sensors and control elements for everyday items such as waste bins or appliances to remotely provide information or automate processes. These applications only require sporadic radio communications with small amounts of data. The radio network for a smart city must connect hundreds or even thousands of identical end-point devices, many of them battery powered.

Such applications were inconceivable when mobile communications were first developed but now define the 5G concept. The main focus has shifted from people to devices or machines and the internet of things (IoT).

➤ Figure. 1: 5G aims to cover three application groups.

KPI	5G	6G
Peak data rate	20 Gbit/s	1 Tbit/s
Average available data rate	100 Mbit/s	1 Gbit/s
Signal latency	1 ms	0.1 ms
Maximum channel bandwidth	100 MHz	1 GHz
Reliability (error-free data blocks)	99.999 %	99.99999 %
Maximum user density	106/km <sup>2</sup>	107/km <sup>2</sup>
Maximum user speed	500 km/h	1000 km/h
Positioning accuracy	20 cm to several meters in 2D	1 cm in 3D

➤ Table 1: Comparison of 5G performance data and KPIs discussed for 6G.



► Figure 2: Augmented reality glasses are already merging real and virtual worlds, but the vision with 6G is to include all senses for total immersion

## The 6G vision

Technical development is closely aligned with the demands of different industries. The visions for 6G vary widely and merge to form a fascinating landscape. Bringing this landscape to life will require evolution of existing technologies but also capabilities that are mostly not yet available, but which are within reach on the medium term. The interaction between all these technologies will create the sixth mobile communications generation, but the term fails to describe the true potential of 6G.

## Digital twins on the holodeck

Facebook founder Mark Zuckerberg announced the metaverse in autumn 2021 and also changed the company name to Meta. With that he gave once gimmicky VR headsets new market relevance. They are the main tool for implementing Zuckerberg's vision of extended reality. The company has the means, since VR headset manufacturer Oculus is part of the Meta empire.

Reimagining the original idea behind the VR headset is ambitious and visionary. Specialists use the glasses, for example, to project a 3D model of a part to be mounted into the real image – together with information on how to handle the part.

The person wearing the glasses can even interact manually with the holographic projection as if it were real. This includes touching and manipulating the projection. Making such a system available in the millions and affordable for everyone is Zuckerberg's vision and one of the guiding scenarios for 6G. Extended reality – the combination of real and virtual worlds – encompasses a number of other substantial visions if taken to its logical conclusion.

Ultimately, the long-term goal is total immersion into a new world that is experienced as if it were real. This includes elements such as three-dimensional optical resolution capable of fully stimulating human eyesight, an appropriate acoustic environment, instantaneous reaction by all synthetic objects (tactile internet) and finally, a credible

representation of all of these things. Some of these objects have to match up with twins in the real world.

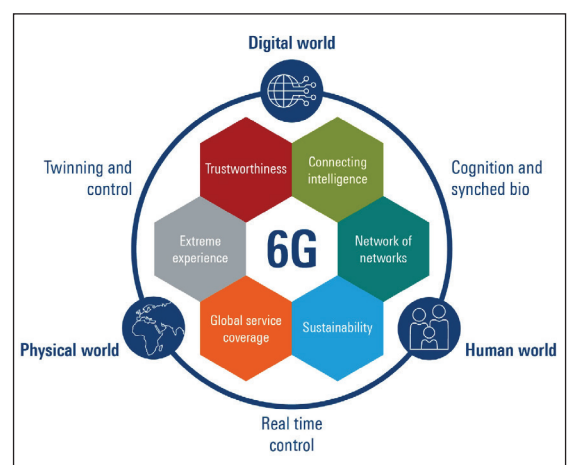
The digital twin is an interactive, virtual representation of a real object or machine that can be manipulated from the metaworld. The ability to operate machines from practically anywhere has potentially far-reaching consequences for the work environment and society at large. One potential impact is the revival of rural areas, since people will no longer need to move to urban areas for work.

When thinking about scenarios like this, you simply cannot ignore 6G. VR headsets do not have the processing power required for the immersive artificial world of the metaverse. And if we want the headset to be compact and look like regular glasses, we need external computing power. If this processing power comes from the cloud, 6G is absolutely necessary.

Transferring extremely large quantities of data to the glasses with video resolutions of at least 8K in stereo requires transport capacities of several hundred gigabits per second along with signal transit times of a tenth of a millisecond to enable natural reactions in real time. 5G does not have the capacity for this. Networks will also need to allocate computing power intelligently for the various 6G services, and this is where artificial intelligence comes in. In fact, AI will be ubiquitous in 6G networks.

## The real internet of things

Although the internet of things is slowly taking shape and industrial and transportation applications have received a boost from 5G, universal connectivity is only possible with 6G. Based on its technical configuration as well as its capacity, 6G should be capable of integrating any number of objects in homes, industries, road transport



► Figure 3: 6G is set to meld the physical world (environment, machines), the digital world (data, virtual environments) and the human world in a symbiotic way, as shown here in the vision presented by the European Hex-X initiative.

or infrastructure. This opens up networking opportunities that were never possible before. Embedded radio sensors can help monitor the condition of bridges and highways, making it easy to see when maintenance is needed. The RFID tags commonly used in retail sales and logistics can only be read from a short distance. Equipped with special sensors and a larger range, however, they could be used to monitor food quality.

The IoT boost will also change how connected radio sensors are powered, which presents a huge challenge for their large-scale deployment. The sheer quantity of these sensors as well as the degree of miniaturization makes it unfeasible to exchange the power cells. Since many applications are conceived for long-term deployment over many years, the sensors must be able to provide their own power. Zero energy devices and energy harvesting are two buzzwords here. Today's RFID sensors work with electromagnetic energy harvested directly from a nearby reader or scanner. But 6G sensors will have to make do without this convenience and obtain power from suitable local sources such as heat, light or motion. As with many other 6G topics, research in this area is still in its infancy.

## A network of radio networks

6G will be not only an inexhaustible basis for the internet of things, but also a new kind of internet. With 6G, fixed, mobile terrestrial and non-terrestrial networks will integrate seamlessly into a constantly changing heterogeneous network landscape (organic network). Commercial, private and public subnetworks of all sizes will coexist, ranging from the macrocells that exist today and provide coverage over an entire square kilometre – to attocells and zeptocells with coverage for a single room or vehicle.

Openness, virtualization and disaggregation are required to tailor network functionality to the customer application and to spark innovation of new services. The disaggregated network's function blocks must provide multivendor support in compliance with the standard. Rohde & Schwarz is an active member of the O-RAN alliance, which is already laying the foundations for this.

## The race is underway

Initial discussions of 6G only began a few years ago, but since then a lot has happened in industry, research institutes and the political world. Research initiatives have been set up around the world, financial support has been granted and alliances have been forged. Politicians understand that competitiveness – and the economic prosperity of their countries – may rest on equal participation in the 6G system while avoiding dependency. In the spring of 2021, Japan and the USA agreed to invest 4.5 billion dollars in 6G research. South Korea has an ambitious plan to invest some 195 million dollars over the next four years and will be ready for preliminary field tests by 2026.

Europe has launched its flagship 6G project, Hexa-X, with organizations from nine different countries. Rohde & Schwarz is actively working with relevant research organizations worldwide. Separately, the German Federal Ministry of Education and Research is providing 700 million euros in funding until 2025. In the short term, 250 million euros will go to four national research hubs where Rohde & Schwarz is involved as a partner or project coordinator.

And then there is China. Of course, China has no intention of giving up its strong 5G position simply because the next generation of technology has arrived. China's Ministry of Science and Technology is working with other ministries and government agencies to coordinate national resources and get 6G ready for deployment as quickly as possible.

● *Rohde & Schwarz has been a close partner to industry as well as a leading supplier of T&M equipment since the very beginning of the digital mobile communications era. The company's products and expertise are already in use today in various 6G research and development projects, and the company is committed to also provide the measuring equipment needed for 6G large scale rollout.*

## 6G Research Areas

There is a need for further research and development in the following areas:

**FREQUENCIES:** 5G is using the millimetre wave range (> 20 GHz) for individual communications for the first time. FR2 (7.125-24 GHz) is the most



➤ Figure. 4: Design study carried out by network equipment supplier Ericsson: zero energy devices can benefit more than just civilization. For example, a 6G IoT radio sensor could measure ecosystem data and transfer it to a processing centre.



promising frequency for mass 6G rollout. But 6G will also use higher frequencies: up to 100 GHz and higher for sensing and 90-170 GHz for backhaul. Even the terahertz range (300 GHz to 3 THz) is being explored.

**ANTENNAS:** at such high frequencies which correspond to short wavelengths, the antennas have dimensions in the millimetre range. Base stations will combine up to 60 000 of these antennas into arrays to supply simultaneous coverage for hundreds of mobile devices via individual directional beams. Reconfigurable intelligent surfaces (RIS) are being developed today. They could be deployed on building walls, for example, to improve the performance of wireless communications in terms of coverage and efficiency.

**ARTIFICIAL INTELLIGENCE (AI):** AI will be a major hallmark of 6G. It bears the potential to dynamically adjust the network to cope with varying environment and customer demand. AI will be used in technical components as well as in network planning and monitoring. The ultimate goal is to achieve a zero-touch (self-optimizing) network in terms of cost, energy, spectral and operational efficiency.

**VIRTUALIZATION:** all of the main network components should be defined and addressable via standardized abstract functions. This ensures that products from different manufacturers can be combined while leaving room for specific technical configurations.

**SELF-POWERED SENSORS:** quantity wise, myriads of miniature sensors will form the largest share of the internet of things. They will need to operate maintenance-free for prolonged periods of time while obtaining power through energy harvesting.

**INTEGRATED RADIO, SENSOR AND COMPUTER NETWORK:** 6G will be much more than just a radio network. Integrated location and sensing functions will allow the position of network users to be pinpointed down to the centimeter while checking his vital functions. The network's processing power will also be massively distributed and harnessed either close to the network user or in remote data centres depending on requirements (edge, fog and cloud computing).

**DATA INTEGRITY:** 6G networks will form the backbone of business and industry – even more than 5G. Countless business processes and services will be based on these networks. Data security is therefore critical. Users must be correctly authenticated with absolute reliability. Every connection will require encryption. Block chain technology is being considered as a way to avoid dependence on central instances in order to ensure data integrity.

**ENERGY EFFICIENCY:** energy demands inevitably also rise when data communications grow exponentially. The energy consumed per bit transmitted needs to fall in order to keep energy efficiency in check.

## Introducing the ET60/ET65 Enterprise Tablets



It's a rugged **tablet**.  
It's a rugged **laptop**.  
It's a rugged **vehicle mount mobile computer**.  
It's **everything** you need...all in one tablet.



For more information, please visit [www.zebra.com/et6x](http://www.zebra.com/et6x)



© 2023 ZIH Corp and/or its affiliates. All Rights Reserved. Zebra and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. 06/05/2023 \* Citizens Band Radio Service (CBRS) only available in the US.

Maximize productivity and business efficiency with the business tablets that deliver more — more features, more power, more security, more ruggedness and more versatility.



**Designed to handle practically everything** — survives more real-world tests than any other tablet in its class



**A display you can see everywhere** — because your workers can be anywhere



**Extraordinary lifecycle** — buy it for 4 years, with available support for 8 years



**It's 3 devices in one** — use it as a tablet, a laptop and a vehicle mount computer



**Trailblazing processor powers it all** — the latest wireless networks and apps



**The most powerful wireless connections** — 5G, Wi-Fi 6E, private 5G and CBRS\*



**Power it your way** — standard or extended removable batteries, or power vehicle mounted tablets with your forklifts



**Barcode scanning at its finest** — standard or extended range scanning to capture barcodes as far as 40 ft/12 m away



**Mobility DNA only from Zebra** — complimentary software tools make Zebra devices easier to use, support and manage

# Realize your company's IT potential

Software to design, monitor, and manage your IT space

62% of IT outages can be attributed to IT infrastructure failure<sup>1</sup>. Our Data Center Infrastructure Management (DCIM) 3.0 offer provides device monitoring, health assessments, and more so you can:

- Run simulated impacts to expose vulnerabilities in IT infrastructure and address them immediately
- Reduce physical threats by monitoring IT environmental conditions
- Improve sustainability efforts by tracking PUE, energy, and carbon emissions

#CertaintyInAConnectedWorld

[apc.com/edge](https://apc.com/edge)



EcoStruxure™ IT  
modernized DCIM

APC Smart-UPS™  
Modular Ultra

<sup>1</sup>Uptime Institute Global Data Center Survey, 2018





## Protecting digital trust from erosion

Every successful IT attack against companies makes consumers doubt whether they want to continue using their data and these services. But data is essential so that companies can digitise their business and develop towards a data economy. Company leaders should rethink and accept that attacks against their IT will be successful. So, what follows from this?

**BY MARK MOLYNEUX, EMEA CTO AT COHESITY**

THE CHILD is crying in their room because the flight that was supposed to bring a parent home in time for their birthday has been cancelled. The airport is locked because the ticketing systems are infected with ransomware. Your most important gift, wisely ordered weeks ago, is still on the way. Unfortunately, not a single ship from the logistics company has been able to leave the ports in Asia for weeks.



All of these attacks happened last year and have been repeated dozens of times in modified form over the past few months. Attacks on the Stade drinking water association, against the health insurance company Barma, the Medical Service (MD) Lower Saxony and Bremen, to name just the most recent incidents. Germany ranks fourth internationally for registered ransomware attacks

between July 2022 and June 2023: the security researchers at Malwarebytes counted 124 such cyber attacks in Germany during the period.

The consequences of such attacks directly affect the lives of every citizen and result in two outcomes: Every citizen understands how many IT-based services they now use - and how much they depend on them. And with every successful attack, a part of the trust that is placed in service providers and their digitised offers is eroded. Anyone who was personally affected by these failures, data losses or other cyber threats will think twice about using new digital offers.

Conversely, companies will be able to generate more sales if their customers trust their digital offers.



This is the conclusion of a McKinsey study of 1,300 business leaders and 3,000 consumers. It shows that companies that are best placed to build digital trust are also more likely than others to achieve annual growth rates of at least 10 percent in their sales and profits.

Other analyses, such as those by IDC also clearly show that companies want to act more and more in a data-driven manner. You want to implement an internal data culture and participate in data management. Sharing data, creating added value for customers and partners and ultimately making more profit. But everything depends on whether customers are willing to share their data and take advantage of corresponding offers.

### Key to the data economy

But consumers have become more sceptical. They are increasingly interested in how companies handle their data. And they assess how companies handle disasters in which data is lost and services are down for a considerable period of time.

The decisive factor here is how transparent and good companies are at explaining to customers exactly what is happening with their data and how. They define a value system and want to know how companies protect their data, how they effectively achieve cyber security and what they plan to do with third parties, especially in the area of AI and data sharing. If one of these sensitive values is violated, trust suffers and customers are reluctant to share data. However, a data economy is absolutely dependent on this data.

Companies rate their ability to stop cyber attacks in time and protect customer data quite positively, as the McKinsey study also shows. Dozens, if not hundreds, of successful attacks on companies worldwide prove every day that there must be a serious gap between self-assessment and real-world capabilities. A loophole through which cyber saboteurs infiltrate, encrypt or steal customer data, thereby challenging the data economy as an idea.

And this gap is getting bigger and deeper because companies are digitising their processes more, trying out more complex services and new approaches like the Internet of Things. These new architectures generate more data in more places. Which challenges the IT teams even more.

### Strengthen resistance

Previous concepts that build additional and higher security walls around data and systems no longer do justice to this new world. Because even the highest wall becomes permeable when employees click on the wrong things, software products have hundreds of vulnerabilities, and remote working has stretched the entire security architecture. Networks, although they are shielded by thousands of individual tools in large companies, have become much more permeable to hackers.

Company leaders should start with the premise that attacks against their company will be successful. This automatically leads to how the consequences of this slump could be contained as quickly as possible. Because, firstly, the most important data should continue to be protected if someone breaks in internally. And secondly, the most important services should continue to function even if a cyber attack starts to rage internally. This is real cyber resilience, and forces companies to modernise their important data management and data security areas in IT.

Such clever new concepts shield the data with strong encryption, strict access controls, isolated data vaults and immutable storage so that saboteurs cannot access it. Even if they have been spying on the victim network for weeks, which is what happens in large professional attacks.

Modern tools help IT and security teams quickly and, most importantly, cleanly recover data and critical services at scale in hours or days. This is where the wheat is separated from the chaff, because old concepts do not examine the data copies and, in an emergency, reconstruct all the data again or the back doors and attack artefacts of the saboteurs, enabling them to break in again within minutes through the same, kindly reconstructed back door. Modern tools, on the other hand, help security teams quickly find and eliminate these artefacts and traces of attacks so that the recovered data is safe.

This makes companies resilient because they quickly contain the consequences of successful attacks and keep their core services available. Their customers' data remains intact and the services remain available, thereby maintaining the digital trust of their own customers.

Such clever new concepts shield the data with strong encryption, strict access controls, isolated data vaults and immutable storage so that saboteurs cannot access it. Even if they have been spying on the victim network for weeks, which is what happens in large professional attacks

# How to cure cloud connectivity headaches with software-defined cloud interconnect



The evolution of cloud technology has left business decision-makers spoilt for choice when searching for the cloud providers that best support their needs. While a wide array of options introduces new and interesting possibilities for organisations, having so many providers to choose from can also be confusing.

**BY PIERRE CÉROU, DEPUTY CTO AT INTERCLOUD**

TAKE A MULTICLOUD arrangement as an example, where monitoring several cloud environments and networks can be hugely complex without end-to-end connectivity and visibility. This can lead to a number of problems, including issues around cybersecurity or compliance with data sovereignty and data protection regulations.



This is where software-defined cloud interconnect (SDCI) enters the conversation. SDCI is central to delivering the security, visibility and network connectivity needed for a multicloud strategy, providing private connectivity to a variety of cloud, network and internet service providers and enabling monitoring of these environments from a single place. SDCI can be implemented as a managed

service, reducing the strain on organisations by delegating complex cloud connectivity responsibilities to a third party.

## The intricacies of cloud networks

Access to multiple clouds can be advantageous for many reasons, but can also lead to a lack of centralised network visibility and control. In terms of security, this makes it more difficult for teams to identify and respond to threats, as well as enforce consistent security policies and configurations across diverse cloud environments.

Maintaining adequate data protection practices and regulatory compliance is also challenging in the absence of end-to-end cloud connectivity. Typically, individual cloud service providers apply their own set of security controls, encryption mechanisms and compliance standards.

As a result, harmonising all of these different protocols and configurations can be a headache for businesses. Failing to adhere to requirements could mean they could fall foul of data protection or data sovereignty regulations, particularly if the organisation operates cloud environments in multiple countries or regions.

## Where does SDCI come into play?

SDCI technology is still developing, but it is already able to support businesses in addressing the above difficulties and achieving greater visibility of their



By providing private connectivity between enterprise sites and cloud service providers, alongside a single interface through which organisations can monitor the performance of each cloud environment, SDCI helps eliminate network complexity.

cloud environments. Its popularity is on an upward trajectory: according to Gartner's 2023 Hype Cycle for Enterprise Networking, 30% of global enterprises will use SDCI services by the end of 2027, up from less than 10% in 2022.

By providing private connectivity between enterprise sites and cloud service providers, alongside a single interface through which organisations can monitor the performance of each cloud environment, SDCI helps eliminate network complexity. The same technology can also interconnect two or more cloud service providers without needing to traverse the internet.

Deeper interconnectivity and greater transparency deliver numerous advantages for businesses. The reliable interconnectivity and visibility that SDCI provides eliminates much of the mystery around multicloud and network complexity. The fact that SDCI delivers private connectivity also ensures better security, as workloads are not exposed to the internet or external threats, and the ability to monitor clouds from a single location means any security issues can be spotted and acted on in good time.

### Barriers to SDCI adoption

SDCI has significant potential, but there are further steps that need to be taken in order to maximise its potential. Many of the barriers to greater adoption revolve around a lack of overall awareness of SDCI's benefits, which can easily be overcome if these advantages are communicated in the right way. Gartner's Hype Cycle report cites a number of challenges. One is a perception amongst leaders that their company only needs to employ internet connectivity directly into cloud service providers. This boils down to many organisations not being aware of the different types of connections into cloud service providers, and specifically the advantages of the private connectivity offered by SDCI.

Another difficulty is that some business leaders remain largely unaware of the availability of SDCI technology, its key benefits and how to adopt it. One reason for this is the fact that SDCI capabilities are evolving rapidly, so it can be difficult to know exactly when to invest in it.

### Bespoke services and streamlined communication are the answer

On the upside, there are many ways we can overcome these hurdles and boost the accessibility

of SDCI for businesses. First of all, we can increase the provision of end-to-end SDCI managed services.

As with other IT managed services, this removes much of the burden and complexity of adopting and adapting to SDCI, delivering more efficient, visible and secure cloud connectivity and all of the benefits mentioned above, alongside ongoing support to make sure the technology is tailored to the needs of the organisation. Advantages include real-time performance and KPI monitoring, as well as full flexibility and control over how users connect to their cloud environments.

Experts in SDCI should also take the time to educate the market about the technology more generally. This involves communicating clearly and concisely about SDCI's functionality, its important benefits and how the technology is evolving. Being conscious of the specific challenges of different industries is also key, as this allows for managed services to be adapted for a wide range of requirements.

The prevalence of SDCI services is growing and will continue to do so. As long as this progress continues in the right way and providers focus on delivering comprehensive managed services to organisations embracing SDCI, the technology will play a defining role in shaping the future of cloud connectivity.





# Disaster recovery is not the same as ransomware planning

Cyber threats continue to rise at an exponential rate in today's digital age. Ransomware attacks are constantly in the news – seemingly on a daily basis.

BY TONY MENDOZA, VICE PRESIDENT OF IT, SPECTRA LOGIC

RANSOMWARE wreaks havoc by encrypting an organization's files, then, the threat actor(s) communicates a demand for a ransom in exchange for decryption of data. While advancements in hardware and software have improved reliability and resiliency, security remains a people problem. Cybercriminals are constantly finding new ways to exploit vulnerabilities and profit from valuable digital data. With ransomware attacks costing companies millions of dollars (the average ransomware cost for an organization is \$4.54 million USD), it's important for organizations of all sizes to understand how to recognize, withstand and recover from an attack, all while maintaining business continuity and rejecting ransomware payoffs.

Last month, the Department of Homeland Security investigated whether security information was exposed in a ransomware attack on the contractor Johnson Controls International. This ransomware attack is a reminder of the importance of

cybersecurity and having a plan in place in the event an attack takes place. Ransomware criminals especially love government contractors, because of the sensitive nature of the data they have – which

increases the likelihood that their demanded ransom will be paid quickly. Ransomware attacks are also becoming more frequent in the healthcare industry for the same reason.

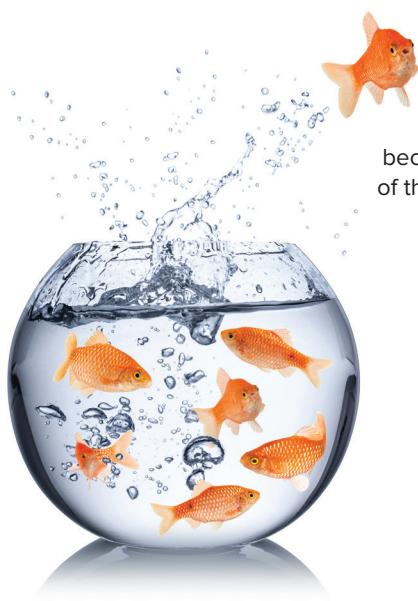
You may have a rock-solid disaster recovery (DR) plan in place, but though disaster recovery is often equated to ransomware recovery, the two are in fact, not the same. Both types of plans aim to minimize the impact of an unexpected incident, recover from it, and quickly restore the organization to its normal production levels.

However, mitigating and recovering from a ransomware attack with a ransomware recovery plan is different than having a DR plan. In essence, disaster recovery is centered around recovery objectives and necessary steps to restore operations after an incident, while the primary focus of a ransomware recovery plan is to safeguard sensitive data during an event. It also defines the scope of action, roles and responsibilities of the incident response team. In fact, the best idea is to have and merge both to create an air-tight strategy that lessens the impact of a cyberattack. Consider what to add to your DR plan to make your infrastructure as ransomware resilient as possible.

Here are some things your organization can do to prepare for and mitigate a ransomware attack:

## Preemptive Steps Against Ransomware

- Develop and test your disaster recovery plan, including a ransomware recovery plan to ensure that the organization is prepared
- Ensure the employee base is well-educated on recognizing email phishing attempts
- Maintain secure backup processes and up-to-date software, following industry-recognized best practices established in the 3-2-1-1-0 rule and employing ransomware prevention measures like anomaly checks



- Mitigate the blast radius by keeping multiple copies of data, in storage locations where the data can be protected and even air-gapped, limiting what the attack can compromise within your infrastructure
- Minimize the amount of data that needs to be immediately restored by moving less frequently used data off primary storage
- Run regular network security assessments to identify any potential weaknesses
- Create a game plan for the immediate aftermath of an attack, including how to recognize and stop the attack
- Consider cyberattack insurance to provide financial coverage for losses and specialized help from on-call cyber experts

#### Post-Ransomware Measures

- Shut down all systems immediately to prevent further damage
- Implement your response plan, including reporting the incident to the FBI or similar federal agency and contacting key personnel
- Assess the full extent of the damage, including identifying the strain of ransomware and finding your last secure backup
- Evaluate your options for recovery, ranging from negotiating with the threat actor to fully restoring your data without paying the ransom, depending on your preparedness
- Establish next steps and future processes to put in place to prevent another attack from happening again

#### Preventing and escaping the ransomware attack loop

One of the unwelcome challenges organizations face in recovering from ransomware attacks is the presence of attack loops. Attack loops occur when the recovery process inadvertently restores the pre-attack generation of backup files that contain the ransomware. This perpetuates a continuous cycle of attacks, rendering file restoration ineffective. To combat attack loops, organizations can leverage anti-ransomware backup software solutions that

Ransomware-resilient data storage solutions like object-based tape are also playing an increasingly integral role in the fight against cybercrime. Modern object-based tape technology that is S3-compatible enables organizations to easily integrate cutting-edge backup software into their workflows while enjoying tape storage's robust data protection capabilities

identify and quarantine malicious code, disabling it during the recovery process.

Ransomware-resilient data storage solutions like object-based tape are also playing an increasingly integral role in the fight against cybercrime. Modern object-based tape technology that is S3-compatible enables organizations to easily integrate cutting-edge backup software into their workflows while enjoying tape storage's robust data protection capabilities. In the fight against cybercrime, exclusive tape features like the tape air gap, which provides an electronically disconnected copy of data, can be an invaluable lifeline in recovering from ransomware attacks.

#### The importance of evolving cybersecurity strategies

It is no longer a matter of if an organization will be attacked but when. With new security challenges emerging daily, organizations must continually evolve their cybersecurity strategies. By implementing these measures, your organization can be better prepared to handle a ransomware attack and ensure a smoother path to recovery. The time is now to create a robust disaster recovery plan melded with a ransomware recovery plan to ensure your organization can get up and running quickly without paying threat actors or losing customers.



## DIGITALISATION WORLD

New product and process development is the foundation for the growth of the Digitalisation World industry.

If you want to highlight the recent important breakthroughs that your company has made, please submit an abstract to:  
**[philip.alsop@angelbc.com](mailto:philip.alsop@angelbc.com)**

It is imperative that Digitalisation World magazine remains a timely resource for this industry, so we are especially interested in highlighting very recent work.

