



DIGITALISATION WORLD

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

ISSUE | 2025

 AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

DIGITALISATIONWORLD.COM

THE TOP THREE MISTAKES FAILING YOUR CLOUD SECURITY



MANAGED SERVICES SUMMIT BENELUX

LIVE

1 JULY 2025

NOVOTEL AMSTERDAM CITY
AMSTERDAM NETHERLANDS

Now entering its 8th year, the Managed Services Summit Benelux has firmly established itself as the premier event for the European IT channel.

The Benelux region, comprising Belgium, the Netherlands, and Luxembourg, plays a critical role in Europe's IT landscape," "The Benelux region, plays a critical role in Europe's IT landscape, with its thriving digital economy, strong focus on innovation, and early adoption of cloud and cybersecurity solutions. The event brings together leading experts in managed services alongside respected industry speakers, all within this rapidly evolving market.

The Managed Services Summit is series of executive-level events, so you know you'll be among the best in the sector, and those featured will explore the latest trends and developments, evolving customer requirements and how to create value through managed services – both for your own organisation and your customers.

INDUSTRY INSIGHTS



Presentations will cover the latest trends, evolving customer requirements, and strategies for creating value through managed services.

BREAKOUTS



Attend a range of sessions led by leading specialists in the field, focusing on technical, sales, and business-related topics.

NETWORKING



Presentations will cover the latest trends, evolving customer requirements, and strategies for creating value through managed services.

INTERACTIONS



Attend a range of sessions led by leading specialists in the field, focusing on technical, sales, and business-related topics.



TO DISCUSS SPONSORSHIP
OPPORTUNITIES CONTACT:



Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0) 1923 690211

Mark Hinds
mark.hinds@angelbc.com
+44 (0)2476 718971

<https://europe.managedservicesummit.com>



ITEUROPA



VIEWPOINT

BY PHIL ALSOP, EDITOR

Global problems need local solutions and IT can help (or hinder)

➤ First up – an apology to all those who were trying to get some sense out of me in the run up to Christmas. I was rather over-optimistic as to how I could combine a month of travelling to see various sons in Australia, with work as normal, the end result being that, I hope for understandable reasons, family took rather more time than I had anticipated, leading to a skeleton editorial service from early December until the second week of the new year.

Anyhow, life is back to normal, whatever that might be as a new US president continues to divide opinion across the globe. And, when it comes to the ongoing melting pot of social media, political extremes, sustainability and culture wars and the overwhelming sense that something, somewhere in the world might have to ‘give’ on a spectacular scale in the next few years to diffuse the social pressures which are building and building as a result of this chaos, it seems that Australia is no different from anywhere else.

Indeed, my visit to the other side of the world served as a timely reminder that, while it might be relatively easy for our political leaders to develop their strategies and policies, the reality is that, across the globe, there are as many different views on what should be our common priorities as there are countries. So, country A, along with countries B and C, might broadly agree on a way forward when it comes to addressing environmental, economic and social pressures, for example, but countries D, E and F will have wildly opposing views of the right way forward.

As a result, my previously shared view that the only credible way forward which best addresses the many challenges facing the global population is a return to much more local,



sustainable ways of life, has been reinforced during my travels. Sending container ships across the oceans to deliver goods which could be sourced much more locally simply does not/can not make sense if sustainability is to be taken seriously, for example (and no more long distance travel for anyone!). Yes, the fall out from this localisation will be profound and far-reaching – but continuing along our current path, thinking that we can both consume more and more and become sustainable seems incredibly illogical.

The jury is out right now as to the role that IT should play in this future. IT consumes masses of power, and looks set to consume even more as AI takes hold. But IT can also save vast amounts of finite resource consumption in so many ways. IT – villain or hero (or both!)? We are about to find out. If all this sounds a touch pessimistic for the new year, apologies, but long distance travel allows for plenty of time for thinking!



18 The top three mistakes failing your cloud security

The majority of the world's data is still stored on-premises (on-prem), meaning valuable information is left vulnerable to physical damage or theft. When implemented correctly, cloud offers a more secure alternative



14 Avoiding 'False Starts'

A guide to successful data and digital transformation

16 Pool your cybersecurity resources to build the perfect security ecosystem

Cybersecurity has never been something to set once and leave running in the background— it is a constantly evolving landscape



20 It's time to overhaul enterprise cybersecurity alerting systems

What every storage admin should know about their SOC

22 How data streaming is solving the AI sustainability puzzle

When we think of artificial intelligence, we rarely think of the physical world. We think of apps and screens, chatbots and virtual assistants

26 AI must start with trustworthy data

The modern workplace is about to be transformed by artificial intelligence (AI)

28 Cost-Effective AI

Prioritising the full tech stack over raw compute



26

30 Generative AI isn't a threat but an essential co-collaborator for IT teams

Organisations are always looking for ways to enhance and improve their IT practices and processes

32 Beyond the golden cages

Modernising testing workflows for agile network innovation

34 Why effective visibility in the cloud is critical: and how to get there

Many IT and Security leaders are confident they're sufficiently secure across their entire IT infrastructure, from on-premises to cloud



30

NEWS

- 06 Data concerns soar as AI surges – 37% of IT leaders identify data quality as major barrier to AI success
- 07 Execs expect outages
- 08 Gap between goals and skills
- 09 IT leaders grapple with security, efficiency, and skills evolution amid digital transformation
- 10 AI regulation, Greentech and NaaS to top the CIO agenda for 2025
- 11 IT professionals recognise lack of gender diversity



09

DW DIGITALISATION WORLD

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

Published by: Angel Business Communications Ltd, 6 Bow Court, Burnsall Road, Coventry CV5 6SP
T: +44 (0)2476 718970 E: info@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 2025. 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)

Data concerns soar as AI surges – 37% of IT leaders identify data quality as major barrier to AI success

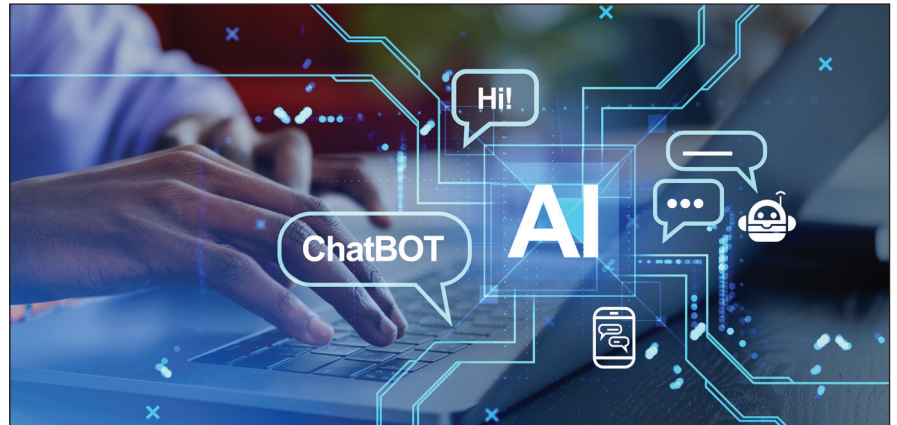
Hitachi Vantara survey finds data demands to triple by 2026, highlighting critical role of data infrastructure in AI success and revealing gaps in data governance, security, and sustainability.

WITH the rapid adoption of AI across industries, nearly two in five (37%) U.S. companies identified data as their top concern when implementing AI projects, but few IT leaders are taking steps to ensure proper data quality and management, jeopardizing the success of AI initiatives according to a new survey from Hitachi Vantara. The Hitachi Vantara State of Data Infrastructure Survey reinforced the critical role that data infrastructure and data management can play in terms of overall data quality and the ability to drive positive AI outcomes.

“Using high-quality data” was the most common reason provided for why AI projects were successful both in the U.S. and globally, with 41% of U.S. respondents in agreement. However, AI has led to a dramatic increase in the amount of data storage that businesses require, with the amount of data expected to increase 122% by 2026. As a result, storing, managing and tagging data to ensure quality for use in AI models is getting harder.

The company commissioned the global survey of 1,200 C-level executives and IT decision-makers across 15 countries, including 250 from the United States and Canada. The survey found that most businesses were focused on security risks at the expense of data quality, sustainability and infrastructure management. Key U.S. findings include:

- Highlighting the disconnect with proper data management, only 38% of respondents say that data is available when they need it the majority of the time. Even less (33%) say the majority of the outputs of their AI models are accurate, and three quarters (80%) say the majority of their data is unstructured, which poses greater risk as data volumes explode.
- Few are taking steps to improve



their data quality: nearly half (47%) don't tag data for visualization, only 37% are enhancing training data quality to explain AI outputs, and more than a quarter (26%) don't review datasets for quality.

- Security is the top priority due to the risks presented; more than half (54%) cited security of data storage as the highest area of concern with their infrastructure, which was 17% higher than the global average (37%). Additionally, 74% acknowledge that a significant data loss could be catastrophic to their operations, while 73% of respondents are concerned that AI will provide hackers with enhanced tools.
- AI strategy is lacking ROI analysis or sustainability considerations, as only 32% ranked sustainability as a priority in AI implementation. Even fewer (30%) said they were prioritizing ROI.
- 61% of large organizations are focused on developing general, larger LLMs rather than smaller specialized models, despite large-scale models being much hungrier than regular models to train, consuming up to 100 times more power.

“The adoption of AI depends very heavily on trust of users in the

system and in the output. If your early experiences are tainted, it taints your future capabilities,” said Simon Ninan, Senior Vice President of Business Strategy, Hitachi Vantara. “Many people are jumping into AI without a defined strategy or outcome in mind because they don't want to be left behind, but the success of AI depends on several key factors, including going into projects with clearly defined use cases and ROI targets. It also means investing in modern infrastructure that is better equipped at handling massive data sets in a way that prioritizes data resiliency and energy efficiency. In the long run, infrastructure built without sustainability in mind will likely need rebuilding to adhere to future sustainability regulations.”

Despite recognizing data quality as the top concern for successful AI (37%) many organizations lack the infrastructure to support consistent data quality standards. More than two-thirds (74%) are testing and iterating on AI in real-time without controlled environments, leaving room for significant risk and potential vulnerabilities. Only 3% report using sandboxes to contain AI experimentation, which raises concerns around the potential for security breaches and flawed data outputs.

Execs expect outages

PagerDuty has released a study that reveals service disruptions remain a critical concern for IT and business executives, with 88% of respondents saying they believe another major incident will occur in the next 12 months.

PAGERDUTY surveyed 1,000 IT and business executives who were director level and above, from the U.S., U.K., Australia and Japan.

The study's findings illustrate how critical it is for companies to implement efficient processes and strategies for preventing major incidents and mitigating damages, while maintaining customer trust.

The PagerDuty study found that the 2024 July global IT outage was a learning experience for organizations. In today's digitally connected world, IT outages can be caused by everything from cyberattacks to human error. 86% of executives surveyed now realize that they have been prioritizing security at the expense of readiness for service disruptions, causing changes within the company. The reality is that a focus on preventing service disruptions, which can often be security-related, is imperative for organizations today.

Preparedness in terms of people, process and culture is key to ensuring disruptions are minimized to limit revenue and reputational harm. 83% of business and IT executives admitted that the July global IT outage caught them off guard, exposing gaps in their preparedness for service disruptions. 89% of executives in the U.K., 84% in the U.S., 80% in Japan and 77% in Australia admit to being surprised by the disruptions.

Nearly half of IT executives (47%) believe that insufficient incident management planning will exacerbate the impact of major IT outages on their organizations, a concern shared by 41% of business executives, if approaches to service disruption are not prioritized.

"The PagerDuty study shows that executives around the globe are



shifting their leadership priorities with major incidents in mind, with 100% of those surveyed reporting a heightened focus on preparing for future service disruptions at their companies," said Eric Johnson, chief information officer at PagerDuty. "CEOs and their boards are now focused on this issue, and with the accelerated pace of AI and other advanced technologies being deployed, companies cannot afford to delay critical technology infrastructure updates."

Additionally, 55% of executives surveyed have observed a mindset shift towards continually evaluating and improving preparedness instead of a one-time move into investments in new systems or protocols that are now complete (45%).

Other key findings from the survey data include:

A strong majority of executives surveyed in the U.K. (91%), U.S. (89%), Australia (88%) and Japan (78%) believe that it's not a matter of "if" but "when" these service disruptions happen. While some organizations were prepared for the digital disruption, others were not. Of those that were not

fully prepared, 37% of executives said the July global IT outage resulted in lost revenue or an inability to process sales transactions and delayed response times by 39% to customer or internal requests.

Organizations that experienced multiple service outages due to the July global IT disruption suffered communication breakdowns between departments (38%), delays in workflow and projects put on hold (35%). Overall, 39% of executives saw an impact on decision-making.

Nearly half in the U.S. (48%), Australia (48%), and the U.K. (47%), along with a majority in Japan (53%) believe that limited access to real-time data tools will further hinder their organizations during an outage, if approaches to service disruption are not prioritized.

For many who experienced disruptions during service incidents, the July global IT outage meant a return to the old ways of doing things, as 44% saw increased reliance on manual processes or workarounds following the incident, showing just how much organizations rely on digital tools.

Gap between goals and skills

Skillsoft has released new research exploring organizations' strategic priorities for 2025 and employees' preparedness to achieve them.

BASED on a survey of more than 2,100 full-time employees in the United States, United Kingdom, and Germany, the findings reveal that less than half (48%) of respondents have been informed of their organizations' strategic goals and priorities for the coming year. Of those that have been informed, only 40% say they are extremely clear about their role in achieving these goals, and just a third believe their skills strongly align with them.

Respondents said improving operational efficiency (48%), increasing revenue and profitability (46%), and enhancing the customer experience (39%) are their organization's top priorities for 2025. The lowest priorities are strengthening data privacy and security practices (17%), closing skill gaps (19%), and improving leadership and management (19%). With this in mind, the top three challenges respondents expect their organization to face next year are talent acquisition and retention (31%), meeting customer expectations and satisfaction (28%), and effective leadership and management (27%). Nearly one-in-four (23%) also anticipate skill and competency gaps.

"Boosting operational efficiency, revenue, and customer satisfaction should undoubtedly be business priorities. However, it is nearly impossible to deliver on these goals without first breaking them down into measurable actions, clearly communicating these actions to their entire workforce early and often, and providing an environment where employees can develop new skills in service of this strategy," said Ciara Harrington, Chief People Officer, Skillsoft. "By creating a strong foundation of talent through training and a consistent strategy communications plan, employees will be better prepared to adapt, innovate, and contribute to their organization's long-term success."



From rapid technological advancements to a new U.S. presidential administration on the horizon, the workplace will continue to shift in 2025, leading to just 23% of respondents saying they feel extremely prepared to handle future work-related challenges.

Contributing to this uncertainty, a fifth of respondents identified the lack of training and skill development opportunities as their primary work-related challenge in the past year. Less than a third (31%) said they had received new training and upskilling opportunities or access to new technologies (e.g. GenAI tools) to achieve their professional goals.

To feel more prepared, respondents are primarily seeking personalized, role-based training options, more frequent and updated training, and access to mentoring and coaching. Beyond preparedness, respondents also saw stronger relationships with colleagues, increased confidence in tackling new challenges, and enhanced creativity and problem-solving skills after training and upskilling.

"Access to training and new technologies nurtures continuous learning and adaptability, empowering employees to tackle future challenges," Harrington continued. "An investment in talent is an investment in the future of your company and its competitive edge."

Clear communication of goals and priorities is essential for organizations to foster workforce confidence and eliminate uncertainty.

Only 25% of respondents are extremely satisfied with their current roles, with those most dissatisfied pointing to feeling unprepared for future challenges (86%) and a lack of visibility into organizational goals (43%). Just 21% of respondents are extremely satisfied with the overall culture of their organization.

Gen Z respondents expressed greater feelings of workplace dissatisfaction (25%) compared to other age groups. 54% of respondents who are dissatisfied with their current roles are somewhat or extremely unsatisfied with company culture.

A majority (81%) of respondents dissatisfied with their role believe their skills are misaligned with their organizations' strategic priorities.

Burnout and exhaustion (39%), decreased motivation/engagement (35%), and overwhelming workload and responsibilities (35%) were respondents' top work-related challenges over the past year. Investing in talent development can help build important time management skills while also providing another opportunity to engage and motivate the workforce.

IT leaders grapple with security, efficiency, and skills evolution amid digital transformation

Cybersecurity, AI, and cloud adoption redefine IT professional roles, reveals Paessler's latest global survey.

THE ROLE of the IT professional is undergoing a significant transformation as organisations face challenges in cybersecurity, artificial intelligence (AI), and cloud adoption, according to a new annual report titled "Paessler Perspectives". Released by Paessler, the report reveals that 77% of IT professionals identify cybersecurity as their top concern, alongside AI (34%) and cloud adoption (27%). The report notes these forces are reshaping the skills, strategies, and priorities required of IT.

Top challenges and strategies
More than 1,500 global IT leaders were asked to rank their top challenges in the next two to three years. Cybersecurity emerged as a top concern at 77%, followed by Artificial Intelligence (34%) and Cloud Adoption (27%). IT teams will be increasingly conscious of cyber threats into 2025, with a single data breach costing organisations an average of \$4.88M, along with irreparable damage to trust and reputation. The shift to cloud, though mitigating some risks, also introduces its own cybersecurity challenges.

"IT professionals are navigating a period of unprecedented change as AI reshapes cybersecurity and cloud requirements, and similarly reshapes IT roles, as teams are required to implement and secure AI-driven tools, automate processes, and address the increased complexity of AI-powered environments," said Martin Hodgson, Director Northern Europe at Paessler GmbH. "These changes emphasise the growing need for IT professionals to develop a mix of technical, strategic, and cybersecurity skills to keep pace with technological advancements."

When asked which strategic approaches their IT operations or monitoring team were considering,



IT leaders stated that automated root cause analysis (46%) and observability (40%) were planned or under discussion. These processes remain critical when it comes to maintaining system health and minimising downtime, especially as cyber threats become more sophisticated. IT leaders now have no option but to ensure cybersecurity is integrated and considered through the entire IT stack, so teams can quickly detect, diagnose, and respond to issues before they lead to serious breaches.

Cloud vs on-premises

The report highlights that 76% of IT infrastructure is still on-premises, indicating a reliance on legacy systems, making it harder to maintain both efficiency and security – especially as the amount of data generated and processed continues to increase. Indeed, over a quarter (27%) stated that cloud adoption will be a top three challenge moving forward.

Encouragingly, most IT leaders are willing to overcome the challenges for the rewards cloud will bring long-term, with 60% of leaders believing that they will transition to the cloud in the next two years. This transition places IT professionals at the centre of managing hybrid cloud environments, and will demand new levels of expertise when it comes to securing, integrating, and optimising both cloud and on-premises systems.

"It's clear that while cloud adoption is recognised as crucial for the

digital transformation efforts and competitiveness of a business in today's landscape, many organisations are still in the early stages of leveraging its full potential," comments Hodgson. "Monitoring tools are essential in this shift, empowering IT professionals to track performance, identify issues, and optimise resource usage – enabling them to balance cost, efficiency, and strategic impact in their evolving responsibilities."

The role of IT leaders in a sustainable future

IT professionals placed sustainability last on the list of potential challenges in the next few years, with just 5% identifying it as a 'top three' priority. What's more, almost half (44%) of respondents are not factoring sustainability into their IT strategies. Yet, with rising regulations, IT leaders must recognise the value of sustainability, particularly in creating energy-efficient, secure infrastructures that optimise and monitor resources in real-time.

For IT leaders who are considering sustainability in their IT decisions, 62% stated that a key benefit was cut costs and increase efficiency in tandem. Meanwhile, 60% believe that sustainability is important on a personal level, whilst 37% of those surveyed stated that management plans to prioritise it.

"While sustainability may not be a top priority right now, we believe it will soon climb the agenda for IT departments everywhere", said Helmut Binder, CEO at Paessler GmbH. "Looking to the future, robust and secure IT infrastructure is essential for achieving business goals, allowing companies to monitor resource consumption and make data-driven improvements that benefit both the business and the planet."

AI regulation, Greentech and NaaS to top the CIO agenda for 2025

Colt Technology Services has released key enterprise technology forecasts and market trends for 2025. Based on its proprietary research among over 1000 global CIOs, and gathered from market intelligence sources, Colt anticipates sustainability-driven innovation, AI regulation and a 'coming of age' for Network as a Service (NaaS) to dominate the enterprise tech leader's agenda over the next 12 months.

MIRKO VOLTOLINI, VP, Technology and Innovation, Colt Technology Services said, "As the new year approaches, IT leaders are stepping forward with cautious optimism, ready to navigate the evolving global economic, political, and technological landscapes after months of uncertainty.

They're looking for new, unique ways to drive sustainability and generate energy efficiency across their infrastructure; they're expecting regulators to build frameworks for AI which protect them but give them the freedom to innovate; and they're exploring the scope and scale of NaaS to secure a market advantage and optimise their infrastructure for AI. The champions of 2025 will be those who are responsible, adaptable, and committed to sustainability."

Tech Trends

SASE and zero trust

Misinformation, disinformation and cyber insecurity are cited within the top

five short-term threats named by the World Economic Forum in 2024. With people and data interacting outside of their network perimeter, enterprises will increasingly turn to Zero-Trust Networking and SASE to create a software-defined perimeter (SDP) to secure their people, their assets and their data. This is compounded by the growing regulation such as NIS2 and DORA. Gartner® forecast that "over the next five years, the market for secure access service edge will grow at a compound annual growth rate of 29%, reaching over \$25 billion by 2027. The underlying SASE products that buyers will use will be split between single-vendor and dual-vendor approaches."

1. Next-generation NaaS

Colt pioneered Network as a Service back in 2017. Since then, thousands of businesses across the world have benefited from the agile, consumption-based network model. Now, the market is more competitive, offering

greater choice and diversity. In 2025 we're likely to see a new era for NaaS as operators build increasingly sophisticated portals with deeper levels of automation and API-access to global partners

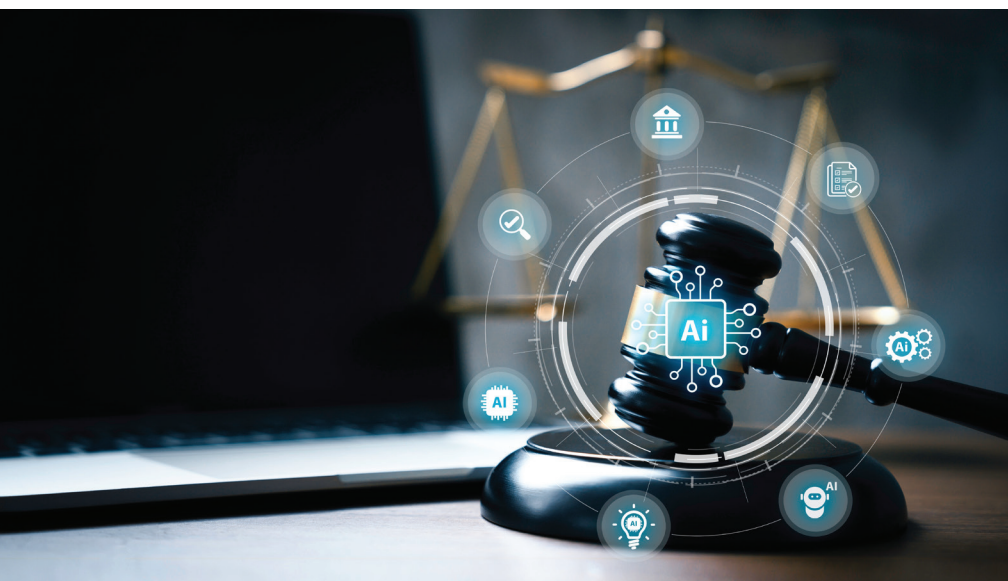
Networks for AI

As more use cases are reaching maturity level, AI is becoming a key driver and enabler within enterprises' digital transformation plans. Gartner forecast that "by 2026 more than 90% of enterprises will extend their capabilities to multicloud environments"

2. The distribution of AI models, enterprise datasets, and IT / OT applications (required for AI training, augmentation and inference) on different public and private clouds is going to challenge the current networking paradigm. We expect to see an increased adoption of solutions incorporating multicloud, high speed, secure and flexible networking capabilities. Inference at the edge will also emerge as a key AI use case, driven by data sovereignty and low latency requirements.

Low Earth Orbit collaboration

With markets likely to encounter socioeconomic headwinds into 2025, businesses will retain a tight cost-control; partnering to expand skills and capabilities is set to continue. This applies across digital infrastructure, as vendors trial new ways to reach customers with secure, low latency infrastructure. One area set to see further collaboration is in the Low Earth Orbit (LEO) sector, as LEO companies plan satellite launches throughout 2025, extending the reach of powerful, high-performance networks bringing connectivity to less accessible areas.



Growth in SDLAN

Traditional Local Area Networks are giving way to Software-Defined Local Area Networks, which offer businesses enhanced security, improved optimisation and deeper levels of automation, while allowing for centralised control of network management. We're seeing them in areas such as manufacturing environments, in which high numbers of IoT devices connect to an SDLAN, and in Financial Services organisations which require the robust protection of sensitive financial data. Growth will continue as we see SDLANs' convergence with Edge driving take-up and AI tools driving optimisation. SDLAN growth will also benefit from the adoption of high speed, low latency, massive IoT capable wireless technology such as private 5G and WiFi7.

Market Trends

Sustainability driving new wave of innovation

Eyewatering power consumption statistics behind AI and large language models have accelerated innovation across Greentech. With 71% of CIOs now responsible for their organisation's sustainability strategies according to Colt's Digital Infrastructure Report, tech leaders will be held accountable for reducing power consumption and meeting environmental and governance targets. These two factors are driving innovation, as tech leaders pilot groundbreaking technologies which are powerful and effective, with minimal environmental impact.

ESG credentials and Scope 3 reporting influencing B2B decision-making

Research in the Digital Infrastructure Report reveals the emerging importance of buyers and vendors in collaborating on environmental and governance goals. 66% of the global CIOs questioned say it is important that a vendor provides services to help them reduce their own environmental impact and 17% would leave their supplier if they did not share their ESG goals. One in five looks to their tech partner for support with their carbon reporting, and 19% for information to help drive Scope 3 reduction. We see this symbiosis continue into 2025 as vendors and partners work together



to drive clarity around reporting and progress towards goals, particularly as non-financial (ESG) reporting is brought up to the same standard and rigour as financial reporting. ESG performance and credentials are being brought to the fore and value chain considerations - including, for example, human rights - will be a key focus, with the right partnerships crucial to compliance and driving positive impact.

AI and the regulatory landscape

From ethical guidelines in Japan and a 'regulatory sandbox' approach in Singapore, to business-friendly AI policies in India and a new EU AI Act in Europe, businesses will be looking to global regulators to provide guidance and clarity around AI as more use cases emerge and countries have a clearer understanding of business and societal impact. New governments coming into power in the US, Europe, Africa and Asia will further influence the regulatory landscape, and IT leaders will be watching and responding.

'AI for good' use cases

Organisations are seeking ways to use AI wisely, sustainably and responsibly. 64% of CIOs questioned in Colt's research say that AI plays a role in supporting or facilitating their environmental impact and governance strategy, and we continue to see examples of positive ways generative and traditional AI models are helping organisations and communities interact with their environment. From utilities firms using AI to collect and

map data on trees in cities such as Singapore to support natural cooling, to businesses using generative AI to support neurodiverse employees with accessibility improvements, we expect to see more positive use cases for AI emerge into 2025.

Telecoms firms retrenching to domestic markets

A wave of incumbents has begun retreating from global to domestic markets, a trend which is likely to continue into 2025 as firms double down on cost reduction. This leaves the market open to truly global operators, and those such as Colt - now the largest pureplay B2B operator in Europe by size, and with infrastructure across Asia, Africa and the Americas - will continue to differentiate on global scale, sustainability credentials and customer experience

Digital sovereignty

The need to safeguard data and secure digital infrastructure is more important than ever before with increasingly-sophisticated threats, a wider attack surface and geopolitical tensions. In the summer of 2024, the UK government classed data centres as critical national infrastructure.

Against this backdrop, digital sovereignty will be crucial as countries look to secure and maintain control over their data and their digital assets. It's a focus we included in our 2024 forecast and we expect it to maintain its presence on the global agenda in 2025.

IT professionals recognise lack of gender diversity

The majority (87 percent) of IT professionals agree that there is a lack of gender diversity in the sector, yet less than half (41 percent) of businesses have programs in place to hire more women, according to new research from ISACA, the leading global professional association helping individuals advance their careers in digital trust fields.

This is despite the fact that ISACA's Tech Workplace and Culture report, which surveyed 7,726 tech professionals around the globe, found that 74 percent of businesses also saying that attracting and retaining talent is a challenge.

When looking at why women are still underrepresented in tech roles, 43 percent of female respondents (and 21 percent of men) say it is because most IT role models and leaders are male. The next biggest culprit was pay inequality, according to 42 percent of women—but only 15 percent of men—who responded.



Overall, men tend to rate their sense of authority in specific areas of their current role more highly, whereas women tend to give lower ratings. The gap between men and women's perceptions of authority are the largest for making purchasing decisions (13 percentage point gap) and contributing to the company strategy and direction (10 percentage point gap).

"More needs to be done to increase the representation of women in the IT and technology sector—and more needs to be done to welcome their leadership and influence," says Julia Kanouse, who serves as Chief Membership Officer at ISACA and oversees the association's SheLeadsTech program. "This will not only help to address the

global skills gap and boost productivity in the sector—it will also create a more inclusive and diverse working environment."

Survey respondents indicate they believe that educational institutions can do more to drive gender inclusion, including:

- Providing mentors or role models (52 percent)
- Establishing tech clubs and/or organizations for networking for women (42 percent)
- Hiring more female tech professors (31 percent)

68 percent of women and 72 percent of men indicate they are extremely or very satisfied with their career progression. Additionally, 73 percent of women and 71 percent of men say they have received a salary increase and/or promotion in the last two years.

Sarah Orton, UK and Europe lead for ISACA's SheLeadsTech initiative, said: "Encouragingly, women have near-equal career progression satisfaction to their male counterparts and are slightly more likely to have received a raise or a promotion in the last two years. Having a workforce of people with different backgrounds, experiences, and perspectives to bring to the table is not only the right thing to do – it's also a business imperative that makes an organization more innovative and it's work that much more efficient and effective. Progress has been made – but the sector has more work to do, and ISACA is supporting this important work."

Half of executives feel overwhelmed by the sheer volume of data and dashboards they receive daily. Only 45% of business data is fully utilised in decision-making, while 34% of business leaders state there simply are not enough hours to analyse the data they receive effectively.

According to new research from TheyDo, business leaders are increasingly dependent on dashboards but drowning in uncertainty due to lack of time to scrutinise data and false confidence in the insights used to inform decision-making. Overwhelmed by the volume of information they receive daily, 77% of executives admit they only sometimes or rarely question the data they rely on daily, despite 67% worrying that over-reliance on static dashboards risks missing critical opportunities.

These are the key findings from Data, Decisions, and Doubt: A 2025 Leadership Perspective, a report based on a survey of 500 senior decision-makers across the US, UK, and the Netherlands conducted by collaborative customer journey management platform TheyDo.

AI promises transformative potential, offering deeper analysis, predictive insights, and enhanced productivity. Business adoption rates are rising steadily alongside fears that unlocking more data and insights will only worsen data overload and exacerbate doubt about the integrity of insights that inform decisions.

The survey discovered high levels of dashboard dependency. Half of leaders confided they feel overwhelmed by the data and dashboards they encounter daily, while most leaders monitor an average of five metrics to measure their department's success. Time is a critical factor, with 34% stating they lack the time needed to analyse the data they receive effectively. Concerns are also high that decisions are made based on false pretences or are misguided, with just 45% of business data fully utilised in decision-making. Collaboration is another weak spot: 41% of leaders admit they rarely involve other departments, leading to fragmented insights and poor coordination.

MANAGED SERVICES SUMMIT LONDON

LIVE

10.09.2025

CONVENE

155 BISHOPSGATE LONDON

Celebrating its 15th year, the Managed Services Summit – London continues to be the foremost managed services event for the UK IT channel.

The UK market remains one of the most mature and dynamic in Europe, with businesses increasingly relying on MSPs to drive digital transformation, cybersecurity, and cloud innovation.

The Managed Services Summit is series of executive-level events, so you know you'll be among the best in the sector, and those featured will explore the latest trends and developments, evolving customer requirements and how to create value through managed services – both for your own organisation and your customers

INDUSTRY INSIGHTS



Presentations will cover the latest trends, evolving customer requirements, and strategies for creating value through managed services.

BREAKOUTS



Attend a range of sessions led by leading specialists in the field, focusing on technical, sales, and business-related topics.

NETWORKING



Presentations will cover the latest trends, evolving customer requirements, and strategies for creating value through managed services.

INTERACTIONS



Attend a range of sessions led by leading specialists in the field, focusing on technical, sales, and business-related topics.



TO DISCUSS SPONSORSHIP
OPPORTUNITIES CONTACT:



Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0) 1923 690211

Mark Hinds
mark.hinds@angelbc.com
+44 (0)2476 718971

<https://london.managedservicessummit.com>

Angel
BUSINESS COMMUNICATIONS

ITEUROPA

ANGEL
EVENTS

The top trends impacting infrastructure and operations for 2025

Gartner, Inc. has highlighted the six trends that will have a significant impact on infrastructure and operations (I&O) for 2025. Gartner analysts presented the findings during the recent Gartner IT Infrastructure, Operations & Cloud Strategies Conference.

“THESE TRENDS give the opportunity for I&O leaders to identify future skills requirements and seek insights to help meet implementation requirements,” said Jeffrey Hewitt, Vice President Analyst at Gartner. “They will provide the differentiation needed for enterprises to gain the optimal benefits from their I&O operations in 2025.”

Trend No. 1: Revirtualization/devirtualization

The recent license changes for certain vendor-based solutions have forced many I&O teams to re-evaluate their virtualization choices with some moving more to public cloud, some turning to distributed cloud and some moving to private cloud. This involves multiple options beyond just changing hypervisors.

“I&O leaders must inventory all current virtualization implementations and any related interdependencies,” said Hewitt. “Evaluate alternative paths including hypervisors, hyperconvergence, distributed cloud, containerization, private cloud and devirtualization. Identify existing I&O skills and how those need to evolve to support top choices.”

Trend No. 2: Security Behavior and Culture Programs

As the sophistication and variety of attacks increases, security programs must evolve to address behavior and culture to optimize their effectiveness.

Security behavior and culture programs (SBCPs) are enterprisewide approaches to minimize cybersecurity incidents associated with employee behavior.

SBCP programs result in improved employee adoption of security controls and reductions in behavior not considered secure. They enable I&O to help support the more effective use of cybersecurity resources by employees.

Trend No. 3: Cyberstorage

Cyberstorage solutions utilize a data harbor made up of data that is fragmented and distributed across multiple storage locations. The fragmented data can be instantly reassembled for use when needed. Cyberstorage can be a dedicated solution with comprehensive features, a platform-native service offering with integrated solutions, or a collection of stand-alone products that augment storage vendors with cyberprotection capabilities.

“For cyberstorage to be successful, I&O leaders should identify the risks of costly and disruptive storage threats, combined with increasing regulatory and insurance expenses to build a business case for cyberstorage adoption,” said Hewitt.

Trend No. 4: Liquid-cooled Infrastructure

Liquid-cooled infrastructure consists of rear-door heat exchange, immersion and direct-to-chip. It enables I&O to support new chip generations, density and AI requirements, while also providing I&O opportunities to flexibly place infrastructure to support edge use cases.

“Liquid cooling has evolved to move from cooling the broader data center environment to getting closer and even within the infrastructure,” said Hewitt. “Liquid-cooled infrastructure remains niche today in terms of use cases but will become more predominant as next generations of GPUs and CPUs increase in power consumption and heat production.”

➤ Figure 1: Gartner Top I&O Trends for 2025. Source: Gartner (December 2024)



Trend No. 5: Intelligent Applications

Generative AI has revealed applications' potential to operate intelligently, which has created the expectation for intelligent applications. Intelligent applications adapt to their user's context and intent, thereby reducing digital friction. It can interoperate in pursuit of their own, as well as their users' intents, by marshaling the appropriate interfaces to external APIs and connected data.

Ultimately, intelligent applications reduce required intervention and interactions on the part of I&O. It also optimizes processes and utilization while reducing resource overhead.

Trend No. 6: Optimal Infrastructure

Optimal infrastructure is when I&O teams place a highly significant emphasis on the best infrastructure choices for a given use case across a range of deployment styles. This approach utilizes a business-based focus so that executives outside of IT can understand why infrastructure choices are made from their perspectives.

"These choices are ultimately aligned with platform engineering adoption," said Hewitt. "They allow I&O to align infrastructure choices with the business objectives of the overall organization. They also facilitate the support and approval of business unit leaders and C-level executives."

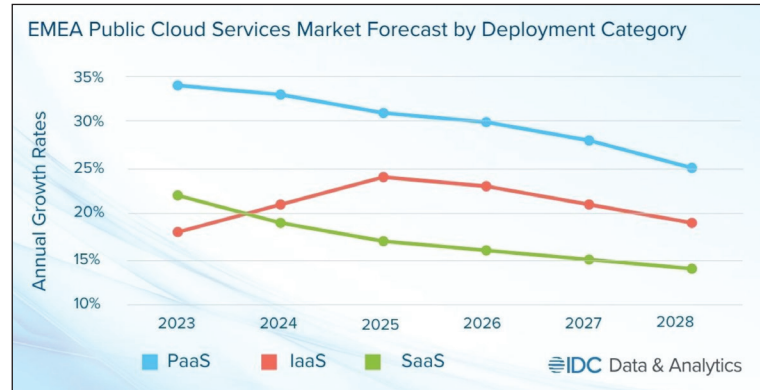
EMEA Public Cloud Services market poised for rapid growth

The Europe, Middle East, and Africa (EMEA) public cloud services (PCS) market, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), is projected to generate \$203.0 billion in revenue for 2024. That's according to the latest Worldwide Semiannual Public Cloud Services Tracker from International Data Corporation (IDC), which forecasts that the EMEA PCS market will reach \$415.1 billion in 2028, representing a compound annual growth rate (CAGR) of 20.0% for the 2023–2028 period.

SaaS, encompassing both SaaS – Applications and SaaS – System Infrastructure Software (SIS), continues to be the largest cloud deployment category, and is projected to make up 64.4% of the total PCS market in 2024.

Due to its size and maturity, SaaS is experiencing the slowest rate of growth among the different cloud deployment models. In contrast, PaaS is the fastest-growing segment, with a projected CAGR of 29.3% for 2023–2028 forecast period, followed by IaaS with a CAGR of 21.6%.

The increased adoption of AI, particularly generative AI (GenAI), combined with ongoing investments in cloud datacenters by global cloud service providers across EMEA, is driving the overall demand for public cloud services. Both end users and technology providers are investing in AI-ready



infrastructures and platforms. Global tech companies will continue to invest in GenAI, embedding more features and functionalities into their existing portfolios. This will create additional opportunities for growth in the IaaS and PaaS markets, boosting adoption of such services across the EMEA region.

"As enterprises adopt GenAI to gain a competitive advantage, the need for scalable, on-demand infrastructure continues to rise," says Manish Ranjan, research director for software and cloud at IDC EMEA. "High-performing compute resources, such as GPUs and other accelerated computing, are essential for running AI/GenAI workloads."

Public cloud service providers are becoming the primary entry point, offering the necessary infrastructure to support GenAI initiatives without significant up-front investments."

From a sub-regional perspective, Western Europe dominates the EMEA market, accounting for over 80% of its revenue, followed by the Middle East and Africa (MEA) and Central and Eastern Europe (CEE). Germany, the U.K., France, and Italy remain the key destinations for cloud investments.

However, global hyperscalers like Google, AWS, Microsoft, and Oracle are aggressively expanding their cloud regions in Finland, Greece, Denmark, the Netherlands, Belgium, Austria, and Spain, boosting cloud adoption across Europe. Similarly, MEA, the fastest-growing sub-region for IaaS, is a hotspot for global cloud providers, with AWS, Microsoft, Google, Oracle, and Alibaba establishing cloud regions in Saudi Arabia, the UAE, South Africa, Qatar, and Bahrain, and planning expansions in Kuwait, Morocco, Kenya, and other tier 2 markets.

AI spending to surpass \$100 billion in next five years

The global Artificial Intelligence (AI) infrastructure market is on track for unprecedented growth, poised to surpass \$100 billion USD in spending by 2028, according to the latest findings from the International Data Corporation (IDC) Worldwide Semiannual Artificial Intelligence Infrastructure Tracker. Organizations increased spending on compute and storage hardware infrastructure for

Source: IDC's Worldwide Semiannual Public Cloud Services Tracker, November 2024

Storage spending in AI infrastructure has been driven by the need to manage large datasets required for training AI models, as well as storage of training, checkpoints and repositories of data for inference phases. This category reported a 36% year-over-year growth rate in 1H24 with 56% of the spending coming from cloud deployments

AI deployments by 37% year-over-year in the first half of 2024, reaching \$31.8 billion.

The AI infrastructure market has sustained double-digit growth for nine consecutive half-years, driven primarily by investment in servers for AI deployments. In 1H24, servers accounted for 89% of the total spending, growing 37% compared to the same period last year.

AI Infrastructure deployed in cloud and shared environments accounts for 65% of the total server spending in AI in 1H24, as hyperscalers, cloud service providers and digital service providers expand their infrastructure capabilities. Traditional enterprises, by contrast, have largely lagged behind in adopting on-premises AI infrastructure.

Servers with an embedded accelerator are the preferred infrastructure for AI platforms accounting for 58% of the total server AI infrastructure spending -- growing 63% in the first half of the year 2024. IDC projects that accelerated servers will exceed 60% of the server AI infrastructure spending by 2028, growing at a 19% 5-year CAGR rate.

Storage spending in AI infrastructure has been driven by the need to manage large datasets required for training AI models, as well as storage of training, checkpoints and repositories of data for inference phases.

This category reported a 36% year-over-year growth rate in 1H24 with 56% of the spending coming from cloud deployments. The United States leads the global AI infrastructure market, accounting for almost half of the total spending in 1H24, followed by PRC (23%), APJ (16%), and EMEA (10%).

Over the next five years, IDC expects the APJ region to grow at the fastest CAGR (20%) followed by the USA (16%), EMEA (13%) and PRC (11%). By 2028, IDC forecast AI Infrastructure spending to reach \$107Bn with servers deployed in cloud environments at 75% of the market total and accelerated servers around 56% of the total market spending.

“IDC expects AI adoption to continue growing at a remarkable pace as hyperscalers, CSPs, private companies, and governments around the world are increasingly prioritizing AI. Growing concerns around energy consumption for AI infrastructure will become a factor in datacenters looking for alternatives to optimize their architectures and minimize energy use” said Lidice Fernandez , Group Vice President, Worldwide Enterprise Infrastructure Trackers.

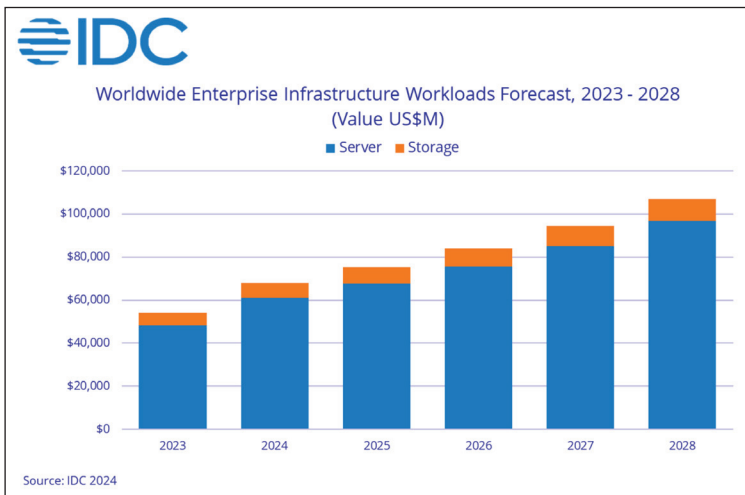
30% of Fortune 500 companies will offer service through only a single, AI-enabled channel by 2028

By 2028, 30% of Fortune 500 companies will offer service only through a single, AI-enabled channel that allows communication through text, image and sound, according to Gartner, Inc.

Multichannel service journeys have become increasingly complex and expensive, leading to a disjointed customer experience and reduced customer retention. Service and support leaders will reexamine omnichannel strategies and leverage advancements in voice-enabled conversational AI to dramatically simplify the service experience.

Instead of offering multiple, distinct channels, a single, AI-powered channel with uninterrupted transitions between different modes of interacting - for example voice, chat, and video - will exist even within the same interaction.

“As GenAI continues to mature and facilitate seamless voice interactions, voice-based customer



service isn't going away. It will instead evolve to meet customers' needs for a more simple service experience," said Patrick Quinlan, Senior Director Analyst, in the Gartner Customer Service and Support practice. "Service and support leaders must pivot from a long-held focus on which channels customers use, to a focus on how customers want to communicate."

Other Gartner predictions to help service and support leaders respond to the changing landscape in 2025 and beyond include:

Seventy percent of customer service journeys will begin – and be resolved – in conversational, third-party assistants built into their mobile devices by 2028.

GenAI has changed the way consumers search for and understand information. In fact, a Gartner survey of 5,459 respondents in August and September 2024 revealed that 45% of customers report using GenAI in their personal life, at work, or both.

With conversational GenAI so firmly integrated into the mobile device experience, customers will self-solve through third-party assistants such as Apple AI and Google Gemini rather than resolve issues through a service organization's official channel.

"Official customer service channels are higher-effort and more complicated, and customers will

be drawn to third-party AI platforms that offer quick fixes and more seamless navigation," said Quinlan. "If a customer can simply ask their phone for the answer, organizations will need to evaluate if their investments in self-service portals are paying off and consider possible customer-facing conversational AI solutions."

By 2027, service organizations will see a 300% increase in fraud attempts over 2023 levels.

Conversational AI tools will appeal to fraudsters who will utilize the same technology to bypass automated systems and deceive live service agents.

To combat this, Gartner expects service and support organizations will develop strategies to counter fraud and protect customers, implementing sophisticated identity verification and multi-layered security requirements for the simplest of interactions.

"It's important to note that though the intention was to reduce customer effort, a single, AI-enabled channel may actually increase efforts and lead to customer churn," said Quinlan. "Leaders will need to balance strategies to reduce effort with those to protect customers from fraud."



DIGITALISATION WORLD

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

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

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



Avoiding ‘False Starts’

A guide to successful data and digital transformation.

BY NIK ACHESON, FIELD CHIEF DATA OFFICER AT DREMIO



IN THE WORLD OF SPORTS, few moments capture the core of false starts better than Usain Bolt’s shocking disqualification at the 2011 World Championships. Bolt’s premature launch in the 100 meters final led to his immediate removal from the race - reminding us that false starts, in any context, can be costly and disruptive.

In an organisational setting, false starts often occur when businesses have to restart their strategy or foundation due to missing any number of key details. Examples of these details may be as simple as discounting the time for security reviews and compliance requirements that impact delivery commitments. It is important to note that quick wins are required, but those wins should be just as foundational as the large and complex ones yet to be prioritised.

“Engineering is easy... It’s people that are hard.” This profound truth encapsulates these challenges perfectly. Organisational limitations and change management need to be at the forefront of a transformation journey. Underestimating this will result in missed deliverables, cost overruns, loss of trust, failed adoption, and inevitably false starts. Businesses that want to not just avoid

this but also stay innovative and competitive, must be proactive and iterative in both delivery and enablement. Just like athletes perfecting their timing, organisations need to ensure they are aligning their initiatives and overall foundational platforms and patterns with their business’ Objectives and Key Results (OKRs): Practicing and preparing every day for whatever the unique challenges that will arise that the pattern still solves.

With aligned patterns, changes in use cases will still utilise the data foundation transformation being delivered. Business priority changes should not impact the foundation. Thus, the team can balance quick wins on the foundation to prove out value, build trust, and momentum, all while in parallel working on more complex and “big win” use cases that take more time and evolve.

Aligning value and cost for a byte of success A crucial aspect when avoiding false starts is ensuring that every transformation initiative is closely aligned with the business’ OKRs. This involves linking technology platform investments into shared OKRs to ensure all investments are tracked towards



achieving the top business goals. An additional way to assure successful delivery is through self-funding. As foundations are rebuilt, data leaders must consider cost savings and other efficiencies available in their ecosystem.

For example, bringing in a new platform will either decrease the burden on another (lowering license costs) or making at least two other platforms obsolete. Specifically, bringing in a better query engine may reduce costs enough to renegotiate other vendor contracts enabling the team to “self-fund” another new platform.

This new platform may later also help deprecate multiple others as it scales and picks up use cases. All this becomes possible without new funding: self-funding as teams stay within their Annual Operating Plan (AOP) budgets. This strategic shift and focus, regardless of the size of efficiencies, enables technology teams to move faster towards value creation and delivery versus being a classic cost center.

Building the foundation for transformation

For businesses that want a successful data and digital transformation, a solid foundation is crucial. This includes setting up modern entitlement services (who has access to what systems and what they are authorized to access), integrating enterprise data catalogs (tracking what data is in the enterprise, who owns the data, and the context around it), and treating data as an asset (managing data like an actual product). Shortcuts are certainly possible to get quicker wins, but a longer-term plan should be in place to maintain flexibility, such as open architectures to minimise the debt and potential switching costs as technology and businesses continue to evolve. Maintaining this balance means businesses may harness technology’s transformative power to drive faster growth and innovation, without sacrificing the future because of material debt taken on to do it.

Even for a foundational platform like a metadata catalog, as part of the overall data catalog capability, telling stories for investments should shift. Narratives may include actual analysts’ headshots from the company seeking to “shop for data”, note how unified analytics and data democratisation is enabled faster with open format migration, and avoiding failed compliance audits and fines resulting from an easier path for integrations with the proposed changes. These stories are paramount to pitching “how” the platform should be built and “how” it’s inefficient today. The impact to the business and end customers is always the “why”. Any supporting data should be in the appendix and may be spoken to as needed. A good story, however, will make the appendix mostly irrelevant.

Crafting stories from digits

Once upon a time, data was viewed as a mere collection of numbers and figures, often daunting

and incomprehensible, let alone debated about how trustworthy they are. However, as businesses have embarked on the journey of digital transformation, data storytelling has emerged as a transformative practice.

Storytelling breathes life into data, turning it into “insights” versus “facts”, with compelling narratives that resonate with audiences and feel more actionable. This goes beyond improving visualisations, but rather crafting a narrative story around the impact that the data driven recommendations will lead to. The story should include more than the forward-looking opportunities, but also include missed opportunities: The impact that could have already happened if the recommended changes were in place for a recent or past business event.

Storytelling humanises data by weaving together insights and trends, peer benchmarks, and use cases that impact the people being engaged that make it personal and persuasive. Visual elements play a massive role in bringing this all together – offering intuitive representations to clarify and simplify messaging that was once more difficult to understand.

It’s no surprise that data-driven stories can boost audience engagement by a staggering 300%. Storytelling empowers the presenter to adjust on-the-fly without losing sight of the goal. This enables better understanding and alignment by maintaining engagement. As a storyteller improves, their potential to achieve trust, alignment, and funding remains unparalleled.

To avoid false starts, data storytelling must go beyond presenting facts; it must elevate to the emotional resonance of business. It’s crucial for businesses since decisions are often not made based solely on “speeds, feeds, and budget”, but rather for strategic direction. Even for a technology vendor, the role of data storytelling with customers helps stay ahead of competition by ensuring the technology is a strategic asset, offering more than just the initial proving capabilities and experiences. Again, every capability from IT to experiences for an end user should be thought of as a foundational step to the next. Present the athlete, or in this case the company or customer, in victory and describe the training program if asked.

Remember, people love top athletes, but rarely care about their workout schedules. Top athletes love the process more than the race, but still need to be there for the fans. Keep and grow the fans.

Change is emotional and hard, and delivering data that elicits the right conscious and subconscious emotions is the art of the storyteller that drives successful and sustained change. Done right, you will avoid false starts. Miss a detail, and even the greatest can be removed from the race.



Pool your cybersecurity resources to build the perfect security ecosystem

Cybersecurity has never been something to set once and leave running in the background— it is a constantly evolving landscape. While the migration of data and applications to the cloud provides numerous business benefits, many organisations struggle to secure their networks against rapidly changing cyber threats.

BY BRIAN SIBLEY, SOLUTIONS ARCHITECT AT ESPRIA

RANSOMWARE attackers have understood the value of targeting smaller organisations and tailoring attacks to take advantage of businesses they believe will pay up immediately (and often with the backing of cyber insurance) rather than invest in defences.

Tight security for data and resources is now the difference between operations running smoothly or being disrupted to the point that businesses are forced to close entirely. But how can SMBs achieve comprehensive security management and threat intelligence on a budget? Partnerships and alliances provide the solution.

Implementing shared threat intelligence across an alliance of cybersecurity experts creates a more robust security approach. Security specialists, such as Sophos, Mimecast and Microsoft can now offer security integration obtained through strategic cybersecurity cooperation, shared telemetry and threat intelligence as the sum of the parts becomes even more significant than the individual offering. This enables the cultivation of a more sophisticated security ecosystem needed to combat the more sophisticated cyber threats we see today.



Integrating with existing solutions for new findings As data is collected and analysed across different parts of the technology stack, ongoing telemetry across the stack gives more significant insights that can be applied to defend your business IT infrastructure effectively. Rather than act in isolated environments, treat your security stack like a constantly evolving ecosystem. It's not just as simplistic as layering one solution on top of another in your legacy infrastructure. Each integration interacts with other elements, analysing weaknesses and aiming to highlight problems as the security ecosystem evolves.

Shared telemetry and threat intelligence gather information about the individual IT components working together as one complete infrastructure, which allows for more thorough data monitoring and analysis. Operators can suddenly see the bigger picture more easily. This isn't limited to significant security platforms but becomes possible with existing vendors offering public API integrations. Mimecast reported that over 200 API integrations are now available as part of their ongoing security ecosystem, which provides even more insight than their already powerful Microsoft

partnerships. Likewise, the partnerships between Sophos, Veeam and Microsoft support this new and more robust approach.

Collaborative threat intelligence with access to expertise

Automated security technology isn't enough to keep up with modern challenges; having expert eyes on your cybersecurity 24/7/365 is necessary and gives businesses the peace of mind that their network is being tightly monitored. However, due to the growing shortage of cybersecurity talent, millions of businesses are now choosing from a far more competitive IT talent pool for roles integral to securing their operations. Limited resources and budgets mean that smaller businesses are more likely to miss out on high-quality professionals.

As cybersecurity leaders already have the first pick of talent and the resources to secure top operatives, smaller businesses can trust their cybersecurity provider to provide the best boost to their cybersecurity profile, rather than hire internal resources. However, cybersecurity information-sharing partnerships take this one step further by combining the top experts across all allied partners, meaning businesses can leverage the best cybersecurity for a collaborative approach to threat intelligence.

As primary targets for cyber-attacks themselves, MSPs have found expert security partnerships offer greater protection against advanced ransomware attacks. This safeguarding then rolls down as part of their offering to their clients. Businesses can rest assured they can have an expert specific to their particular security issue ready to support them, rather than needing an in-house IT security operator with advanced expertise in all security technologies. The value of this specialist knowledge cannot be underestimated.

Integrate with your cloud backups to safeguard against disruption.

IT security company Sophos reported that 94% of ransomware victims in 2023 had cybercriminals targeting their cloud backups, with 57% of these backup compromise attempts being successful. Ransomware and payment demands were also found to double when successfully compromised, meaning that ongoing preventative cybersecurity strategies are no longer as simple as relying on just a singular backup solution.

Utilising immutable cloud backups should be a core focus for any business' security strategy in 2024. By relying on the integrations of high-profile and industry-respected partners, such as between Sophos and Veeam, or most recently Veeam and Microsoft, companies gain the greater peace of mind that multiple expert eyes keep your data secure. Unified management across solutions ensures they work hand in hand rather than at odds; giving a greater return on investment from the word go

As primary targets for cyber-attacks themselves, MSPs have found expert security partnerships offer greater protection against advanced ransomware attacks. This safeguarding then rolls down as part of their offering to their clients

rather than worrying you're leaving the door open to attack as more security tools require greater management.

Stay focused on your customers – leave the heavy security lifting to someone else

Understanding which solution is best for your business may appear daunting at first, but that's also where an MSP can step in to provide advice. By tailoring the solution to your specific needs, you can be assured you are not buying services you don't need and can trust that the heavy security lifting is in the hands of the right experts, and most importantly, the experts that are sharing their security knowledge for a united approach to threat intelligence.

With the greater power of allied resources and backing, business owners have the numbers when it comes to fighting the ongoing war on cybersecurity. Business owners can leave security to someone they can trust, meaning they can focus on what they do best—their business. They spend fewer hours worrying about ongoing security threats and more time can be focused on what will make their business thrive.



The top three mistakes failing your cloud security

The majority of the world's data is still stored on-premises (on-prem), meaning valuable information is left vulnerable to physical damage or theft. When implemented correctly, cloud offers a more secure alternative. Plus, an additional cloud backup of any data stored on-prem provides a safety net against physical risk. As more business leaders recognise the value of cloud storage and begin to migrate their company's data it is important they prioritise securing their cloud backups as part of that process.

BY JON HOWES, VP AND GM OF EMEA AT WASABI



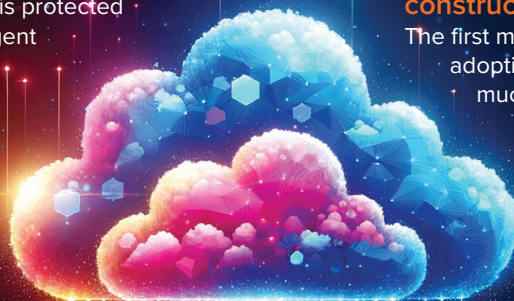
CLOUD is by no means immune to hacks, in fact recent research from Thales revealed cloud resources to be the biggest target for cyber-attacks, with SaaS applications (31%), cloud storage (30%) and cloud management infrastructure (26%) topping the list. However, if migrating to the cloud is done with a security-conscious mindset there are numerous steps that can be taken to ensure your data is protected by the most stringent defence possible.

By neglecting cloud backups business leaders compromise

their sensitive customer data, which may result in legal persecution, financial loss and damaging trust and reputation. The consequences can be dire, so learn from the mistakes of others to reinforce your own business' cloud storage and valuable data found within.

Overlooking the impact of a carefully constructed strategy

The first mistake business leaders make when adopting cloud technology is doing so without much thought. Cloud backups work best when implemented within a well-considered strategy, with rationale and next steps in place. To ensure you are getting the most from your cloud service provider and that your backups are provided the best



possible protection, it is crucial to understand the nuances of cloud technology and its potential risks.

Not all cloud providers are made equal, so selecting whichever big-name appears first from a Google search would be a mistake. Cloud storage companies differ from one another in their security protocols, data handling practices, and recovery options. Do your research and make the choice based on which suits your business' specific backup requirements best. For example, consider how much data your organisation needs to store, in what ways that data will be used and your budget for doing so.

A comprehensive cloud storage strategy will encompass regular reviews, frequent testing and adjustments for evolving business needs like changes to capacity, access methods or degree of security depending on new regulatory mandates.

Part of your strategy should include how frequently backups are completed. A good balance lies between not backing up so regularly that you consume unnecessary storage space but often enough to avoid data loss. A backup is only useful if you know how to restore it; it is therefore crucial to have a strategy in place for restoring the backup quickly and effectively to ensure operations are resumed with minimal disruptions.

Failing to implement strong security

Once you are confident in your understanding of a backup strategy, the next step is to protect your cloud with a suite of stringent security parameters. According to data from the Information Commissioner's Office, the UK was impacted by more ransomware attacks last year than in all previous years combined. Hackers will often attempt to delete your backups in a ransomware attack to prevent you from recovering any data; it is therefore more important than ever to secure your backups.

The first security measure in place should always be multi-factor authentication (MFA). It is necessary to prevent unauthorised access even when log-in details are compromised. Then, encrypting your backup can also prevent unauthorised access. Also, immutable backups — that no user, administrator or third party can delete or corrupt — in the cloud are a proven ransomware mitigation strategy for ensuring that no one can alter or remove your data. Finally, if a cloud provider prioritises security, they would have begun to offer (or currently be developing) multi-user authentication (MUA). MUA means that if a hacker attains the account holding the immutable backups, they will not be able to delete your stored data without additional authorisation from your chosen security contact.

Failing to have these security measures in place leaves your company's data exposed to breaches— with today's threat landscape spearheaded by AI only exacerbating vulnerabilities. A single layer of security is no longer sufficient. When implementing

security measures, it is always best to be proactive; building an impermeable foundation of protection as opposed to patching up the holes after the fact.

The combination of MFA, encryption, immutable backups and MUA creates the strongest barrier we currently have available. It is always worth going the extra mile when protecting your company's data. This ensures you can reconstitute back to your production servers after a cybersecurity incident or accidental data loss, and that you will not have to pay any ransom.

Forgetting about your storage capacity

One of the most simple but frequent mistakes made by cloud users is overestimating the capacity of their storage. The way we talk about the cloud often misleads users into thinking it is limitless; however, your backup capacity is capped by your budget. It is easy to forget when your cloud is due to run out of storage but doing so risks the loss of important data. What's more, scrambling to secure extra storage space at the last minute will likely come at an additional cost, not considered in the budget.



To avoid this, storage capacity must be considered as part of a business' overall cloud strategy. Forecasting growth, understanding your company's capacity requirements and predicting when your use will ebb and flow will ensure you have enough space for continuous backups. Simultaneously, it also helps a company avoid paying for unused space and wasting resources.

Cloud backups can quickly turn from a business assistance to a burden if not approached correctly. Learning from the mistakes of others and understanding where things may go wrong allows you to optimise your cloud storage in a way that best suits your business needs. Thoughtfully constructing a backup strategy involves proactively incorporating security measures and considering capacity requirements. By doing so you can rest assured in the knowledge that you are getting the most from your provider and are protected not only against bad actors but also the easy slip-ups from your own team.



It's time to overhaul enterprise cybersecurity alerting systems

What every storage admin should know about their SOC.

BY ERIC HERZOG, CHIEF MARKETING OFFICER, INFINIDAT

STORAGE ADMINISTRATORS bear a lot of responsibility for their enterprise's data. Some would argue this is one of the most challenging aspects of the administrator role. As soon as the security team gets any indication that a cyberattack may be occurring, a phone call is immediately made to the storage admin, alerting them to the threat. It's all part of ongoing, reactive efforts to protect the enterprise's mission and business-critical data. Precious minutes and seconds tick by, as this manual cyberattack warning system gets underway. The storage admin just has to stop whatever it is they are doing and focus on the fact that a cybersecurity incident could be underway.

When this happens, storage administrators need to be 'firing on all cylinders,' asking the key questions and ensuring the right outcomes. And in these situations, there is really only one right outcome - that enterprise data, lifeblood of all organisations today, is properly safeguarded. But will the storage admins have been quick enough to respond? Will they have succeeded in taking an immutable snapshot of all the data during that split second window? Can all the data be recovered rapidly in the event of a ransomware attack or another type of malware incident?



Hanging in the balance is their entire enterprise's data infrastructure security. Can the storage admin guarantee that a known good copy of the data is recoverable? When one examines the critical

stages in this process it's clear that a great deal of responsibility is resting on the shoulders of storage administrators and their ability to make lightning fast reactions. Is that even possible? What if something else goes wrong? Automation has crept into just about every other aspect of enterprise IT, so why is it that this process and one where the stakes are especially high, is still operating in a silo and dependent on manual intervention?

The reality is that without a fully automated process to capture immutable snapshots of the data before it gets encrypted, corrupted or taken hostage through a ransomware attack, the reaction time is, most likely, simply too slow. Cyberattacks happen so fast, that the loss of even seconds to reaction times can make a significant difference to whether an enterprise can resist, withstand and recover with any certainty. And instead of being heralded as a hero, the storage admin could be slated for poor performance in the aftermath of a security incident. Is that even fair?

How could the enterprise cybersecurity alerting process be improved?

One way to ensure a more dynamically cyber resilient storage infrastructure and improve security of the entire data centre as a whole, would be to seamlessly integrate automated cyber storage capabilities into an enterprises' Security Operation Centre (SOC). Currently, this lack of integration is the missing link between data storage systems and

enterprise cybersecurity. In order to reach this point, the role of storage admin needs to gain a greater organisational appreciation. And CTOs, CIOs, and CISOs will need a deeper understanding of SOCs and how, by linking existing security systems with enterprise storage, they can give their organisations an immense advantage when it comes to recovery from a somewhat inevitable cyberattack.

A SOC has many applications, but is broadly designed to ensure that an enterprise has the most coordinated and effective capabilities for cyber threat detection and response, as well as cyberattack prevention. As most IT professionals know, a SOC is dedicated to monitoring the enterprise's entire IT infrastructure – and they do it seven days a week, 24 hours a day, 365 days a year. It is supposed to detect and respond to any security-related incident in real-time. IT is continually analysing threat data but are missing a trick when it comes to integrating SOC and storage systems.

Enterprise storage needs to be tightly integrated into a SOC strategy, because the SOC is a control centre and unifies all the cybersecurity technologies, including the emergence of cyber resilience tech. Rather like the conductor of an orchestra. And now, due to new technological innovation, cyber resilient storage capabilities can help reduce the threat window – if the alerting triggers the right split second protection mechanisms.

What if a trigger can be defined for cyber storage to proactively take action based on a security incident?

An enterprise's security team can put all its information from security operations through an enterprise storage intelligence grid to create highly sensitive triggers that may otherwise get missed by existing technologies and techniques. IT solution providers have identified this ability to automate data snapshot commands and data pathways as

critical to early detection and worry-free cyber recovery that minimises the effects of even the most vicious and deceptive cyberattacks of malicious actors. There are three 'must haves' to guarantee rapid action:

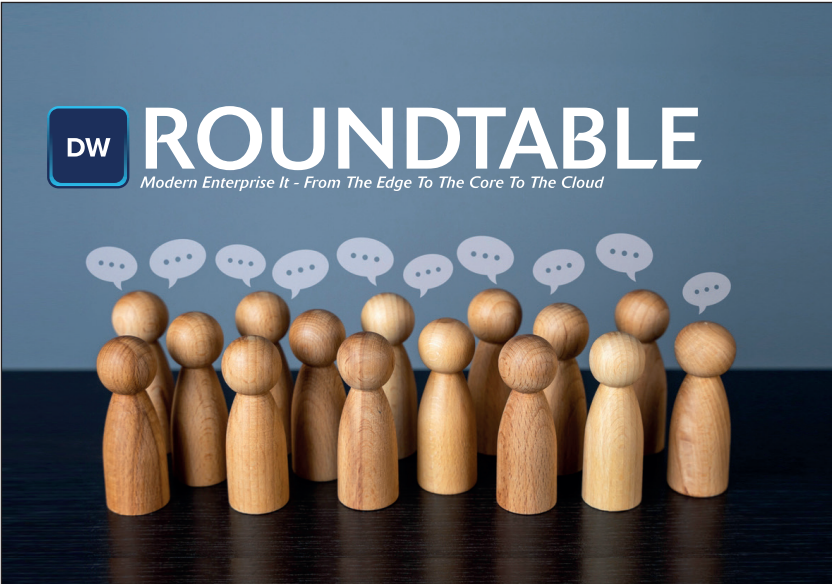
Your enterprise needs automated cyber protection, utilising triggers that security teams define based on security incidents. These may even be barely detectable aberrations that require a deep scanning of the cyber infrastructure.

You need an enterprise-wide cyber storage capability that orchestrates the automatic taking of immutable snapshots of data, at the speed of compute, to stay ahead of cyberattacks by creating a cyber realm to cut off the proliferation of data corruption.

You need an automated cyber protection solution that seamlessly integrates into SOC environments to add a powerful cybersecurity capability to an infosec teams' toolbox in the security infrastructure. It enables more dynamic monitoring that speeds up response to the start of a cyber issue and enables a "handshake" between monitoring for security incidents (the event) and expressing the fabric of core storage – the data (the outcome).

This integration of cyber resilient storage into SOC needs to be considered mission critical because the stakes are simply too high. It extends our thinking beyond traditional enterprise storage to span the layers of cyber infrastructure that need to be reshaped for today's emerging cyberattack vectors and more sophisticated AI-driven infiltration designed to inflict harm to enterprises.

Today it's less a question of 'if' a cyberattack will take place and rather a matter of 'when.' It's time for enterprise storage to stop being relegated as a backroom function and it's time to 'put a SOC' into it.




DW **ROUNDTABLE**
Modern Enterprise It - From The Edge To The Core To The Cloud

- 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 editor, Phil Alsop, this can include 3 speakers
- Questions prepared and shared in advance

Cost: £6995

Contact: Jackie Cannon
jackie.cannon@angelbc.com



How data streaming is solving the AI sustainability puzzle

When we think of artificial intelligence, we rarely think of the physical world. We think of apps and screens, chatbots and virtual assistants. What we don't think about is the 11,000+ data centres around the planet, packed full of server racks, cooling systems, and enough cabling to wrap around the world multiple times over.

BY RICHARD JONES, VP SALES NORTHERN EUROPE, CONFLUENT



TODAY'S data centres consume around 200 million gallons of water per year, while the AI industry uses more energy than a small country. For businesses that have commitments around sustainability and carbon reduction, that poses a serious problem.

While there's no denying the world will continue to need new data centres, there is also growing demand to maximise the capacity that we already have available. By optimising existing space and data processing techniques, businesses can start to do more with less — maximising the advantages of AI without abandoning their existing infrastructure, or significantly increasing their carbon footprint.

This article will explore that idea, and how the recent shift towards data streaming is helping to

solve the 'AI-sustainability puzzle', making AI more efficient, more sustainable, and more powerful for businesses.

The rise of AI

AI might not have taken all our jobs yet, but it's certainly captured the minds of the nation. Research suggests that 56% of young people in the UK have used AI in their workplace, while 36% of the UK population have used Generative AI.

With this explosion in AI uptake, the network itself is starting to feel the strain. As business and consumer demand skyrockets, John Pettigrew, Chief Executive of the National Grid, has suggested that data centre power usage will "surge six-fold in ten years," with £58bn in investment aiming to solve the issue.



MANAGED SERVICES SUMMIT NORDICS

LIVE

21.10.2025

STOCKHOLM WATERFRONT CONGRESS CENTER

Returning for its 2nd year, the Managed Services Summit Nordics builds on the inaugural event's success, offering a premier platform for networking and insightful presentations from industry leaders across the Nordic region.

The Managed Services Summit is series of executive-level events, so you know you'll be among the best in the sector, and those featured will explore the latest trends and developments, evolving customer requirements and how to create value through managed services – both for your own organisation and your customers

INDUSTRY INSIGHTS



Presentations will cover the latest trends, evolving customer requirements, and strategies for creating value through managed services.

BREAKOUTS



Attend a range of sessions led by leading specialists in the field, focusing on technical, sales, and business-related topics.

NETWORKING



Presentations will cover the latest trends, evolving customer requirements, and strategies for creating value through managed services.

INTERACTIONS



Attend a range of sessions led by leading specialists in the field, focusing on technical, sales, and business-related topics.



TO DISCUSS SPONSORSHIP
OPPORTUNITIES CONTACT:



Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0) 1923 690211

Mark Hinds
mark.hinds@angelbc.com
+44 (0)2476 718971

<https://nordics.managedservicesummit.com>

Angel
BUSINESS COMMUNICATIONS

ITEUROPA

ANGEL
EVENTS

Everyone needs to do what they can to reduce that pressure – which means that any business has an obligation to reconsider how they treat, store, and use their data, and how it can be improved. It might not be the be-all and end-all, but incremental improvements can lead to genuine progress, and allow data centres to focus more on their own efforts.

Bad batch

One change that's set to make a major difference to both to the efficiency of data centres and to the power struggles they're wrestling with is the abandonment of batch processing as the dominant means of wrangling data.

Batch processing is just as it sounds: the collection of data into huge storage repositories, which can then be cut and interrogated as needed. This processing often takes place during 'downtime' – for instance, data being collected throughout the day and then processed and analysed at night.



While it's a well-established practice, batch processing has some fairly obvious limitations:

Latency can be minutes, hours, or even days, rendering many results redundant by the time they're received – which is a waste of the power being used to process them, and necessitates further batches.

When interrogating large bodies of data, it's inevitable that unnecessary data within a batch will get dragged into processing, wasting power and time.

Regardless of how successful the processing is, it necessitates power-intensive storage and processing hardware.

In other words: the de facto mode of data processing for most AI is inefficient, cumbersome, and power-hungry. The conventional approach not only fails to prioritise sustainability, but often fails to deliver on performance, too.

Go with the flow

The alternative that flips many of these concerns on their head is data streaming.

Rather than collate and store huge bodies of data only to dredge them back up when they're of use, data streaming processes each individual data point in near-real time, as it enters the system, within the context of the relevant data that has come before.

This means that actions are taken in milliseconds, based on data that is more accurate than batch processing. At Confluent, we refer to this as 'data in motion' – the organisation and activation of data even as it's moving through the system.

It also eliminates the latency of batch processing, as well as more effectively cleaning the data as it enters the system – meaning that any repositories are comprised of more accurate and more timely data than a batch alternative, and thus more efficient to use.

On the hardware front, data streaming can be conducted entirely through the cloud, on-premises, or hybrid, offering serious flexibility from a hardware budget standpoint. And those data stores are either cheaper, or more cost-effective, than a batch equivalent.

All of this speaks to a more sustainable basis upon which data processing can not only run but see a marked improvement in performance. So, to circle back – what does this mean for the data centres in the age of AI?

Looking forwards

A shift towards more sustainable operations will allow data centres to run more efficiently, getting more from the power that's available to them. With companies taking care of their end of the bargain, those data centres are more able to explore opportunities to refine their own ways of working, as less emergency surgery is required to keep things afloat as they are.

Some of that will be a simple refinement of day-to-day operations in the data centre. As AI becomes more ubiquitously available, we're likely to see data streaming uptake right across the data centre space.

It also allows data centres to focus on more creative elements of sustainability that pass on benefits to the immediate community around them. Over 10,000 homes in London can benefit from the waste heat of data centres, which helps to provide heating and hot water; data centres in Sweden and France have used it to cultivate greenhouses.

Ultimately, it's the incremental improvement of companies when it comes to sustainable operations that allow this experimentation, and alleviates the required pressure on the data centre to help facilitate it. A shift from batch processing to data streaming not only delivers this, but adds genuine performance improvements into the bargain.

MANAGED SERVICES SUMMIT MANCHESTER

LIVE

18.11.2025

MANCHESTER CENTRAL
MANCHESTER UK

Now in its 6th year, the Managed Services Summit Manchester continues to complement its sister events in London, Stockholm, and Amsterdam, serving as a premier event for the UK, Nordics, and European IT channels.

The Northern UK market offers unique opportunities and challenges, emphasizing cost-efficiency, practical innovation, and long-term partnerships, making it particularly relevant for MSPs and IT providers.

The Managed Services Summit is series of executive-level events, so you know you'll be among the best in the sector, and those featured will explore the latest trends and developments, evolving customer requirements and how to create value through managed services – both for your own organisation and your customers

INDUSTRY INSIGHTS



Presentations will cover the latest trends, evolving customer requirements, and strategies for creating value through managed services.

BREAKOUTS



Attend a range of sessions led by leading specialists in the field, focusing on technical, sales, and business-related topics.

NETWORKING



Presentations will cover the latest trends, evolving customer requirements, and strategies for creating value through managed services.

INTERACTIONS



Attend a range of sessions led by leading specialists in the field, focusing on technical, sales, and business-related topics.



TO DISCUSS SPONSORSHIP
OPPORTUNITIES CONTACT:



Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0) 1923 690211

Mark Hinds
mark.hinds@angelbc.com
+44 (0)2476 718971

<https://manchester.managedservicessummit.com>



ITEUROPA





AI must start with trustworthy data

The modern workplace is about to be transformed by artificial intelligence (AI).

BY PAUL SCOTT, CHIEF TECHNICAL OFFICER AT MATRIX BOOKING

ALREADY, AI is being used to automate repetitive tasks like data entry and scheduling, freeing up humans for activities that require complex decision-making, emotional intelligence and creative thinking.

Not only that but AI is set to make our office lives easier by spotting problems that slow us down and simplifying our work processes. Imagine it automatically reserving meeting rooms and allocating necessary resources based on real-time needs. It'll be like having an all-knowing office assistant who prepares everything behind the scenes, allowing us to focus on the more critical tasks at hand.

However, this rosy future hinges on one crucial element: trustworthy data. AI algorithms act like complex sieves, sifting through vast amounts of information to identify patterns and make suggestions for improvements. But the quality of these recommendations is directly tied to the quality of the data they're based on.



Improving the workplace with AI

AI in workspace management could fine-tune every area and support employees in meaningful ways. Imagine a system where a person allows it to learn their working patterns. It would be able to suggest

the best resources for when and where they want to work. With this personalised approach, employees would have what they need, when they need it, reducing waste and saving time.

Using real-time data, AI could make immediate adjustments to the workspace. If a meeting room is booked but remains unused, the system can free it up for others. It could allocate desks based on who is in the office that day so that departmental team members could sit next to one another.

On top of that, AI could be integrated with environmental sensors and other building systems to regulate energy usage and make the workspace more comfortable. For example, the system could manage air conditioning or heating based on both planned and actual occupancy. Using this information, it would pre-cool or pre-heat specific areas of the building accordingly. As the working day unfolds, the system would then make real-time adjustments based on occupancy data to maintain a comfortable environment.

In the long term, AI could analyse data trends to forecast future needs. It might predict peak times for resource use and suggest adjustments to meet demand. This would help businesses plan better

and stay one step ahead. The potential for AI to become a powerful tool to optimise the workspace and support growth is clear.

However, if any of the underlying data is flawed, the AI systems will end up taking the wrong actions. As the saying goes – ‘garbage in, garbage out’.¹

The hidden danger of bad data

Collecting accurate data is more challenging than it seems. Decision-makers might think they are getting the right data, but issues like employees booking resources and not using them effectively can create false records. These inaccuracies can make the data seem reliable when it’s not.

Imagine employees book desks for the day, but then spend most of their time in meeting rooms. The resource management system, seeing the desk bookings, might assume full occupancy and not free up those desks for others who need them. This can lead to inefficiencies and frustration, as available resources are misallocated.

A clearer picture could be formed with more nuanced data that combines planned desk bookings with actual occupancy sensors. The system could then make better decisions and optimise resource usage more effectively.

This is just one example of how poor data can turn a well-intended AI solution into a source of problems. Trust evaporates quickly when AI recommendations consistently miss the mark, which is why prioritising data quality is paramount. We need accurate, complete and unbiased data to help AI become a valuable partner, not a source of wasted resources, increased costs and disgruntled employees.

Getting the right data for AI

The collection of trustworthy data starts with encouraging the proper use of booking and check-in systems. Employers must provide regular training sessions to emphasise its importance and make sure everyone understands best practices. Making the booking and check-in process as easy as possible is key.

On top of that, technologies such as sensors can passively collect anonymous usage data, complementing booking information and making it simple for employees to effortlessly engage with the system.

Businesses can also use additional technology to verify check-ins and presence in the office. If someone isn’t present, the system can free up their booked resources for others. This helps maintain accurate data and enables AI to optimise the workspace effectively.

To get the most accurate and complete data, businesses should adopt uniform data collection



methods across the entire organisation. This simplifies data gathering and makes AI insights reliable and consistent. However, large-scale data collection comes with risks, so it’s important to limit access to authorised personnel to prevent accidental or malicious alterations, or unauthorised people getting hold of booking data that could reveal an individual’s booking data and their whereabouts. Protecting data confidentiality and integrity is fundamental to the trustworthiness of AI applications.

Furthermore, clear communication about how data is used and stored builds trust and encourages responsible data management. When employees understand the importance of data security and accuracy, they are more likely to handle data responsibly.

The use of the data can also improve employees’ engagement with the system. Both of which support the overall reliability of AI systems.

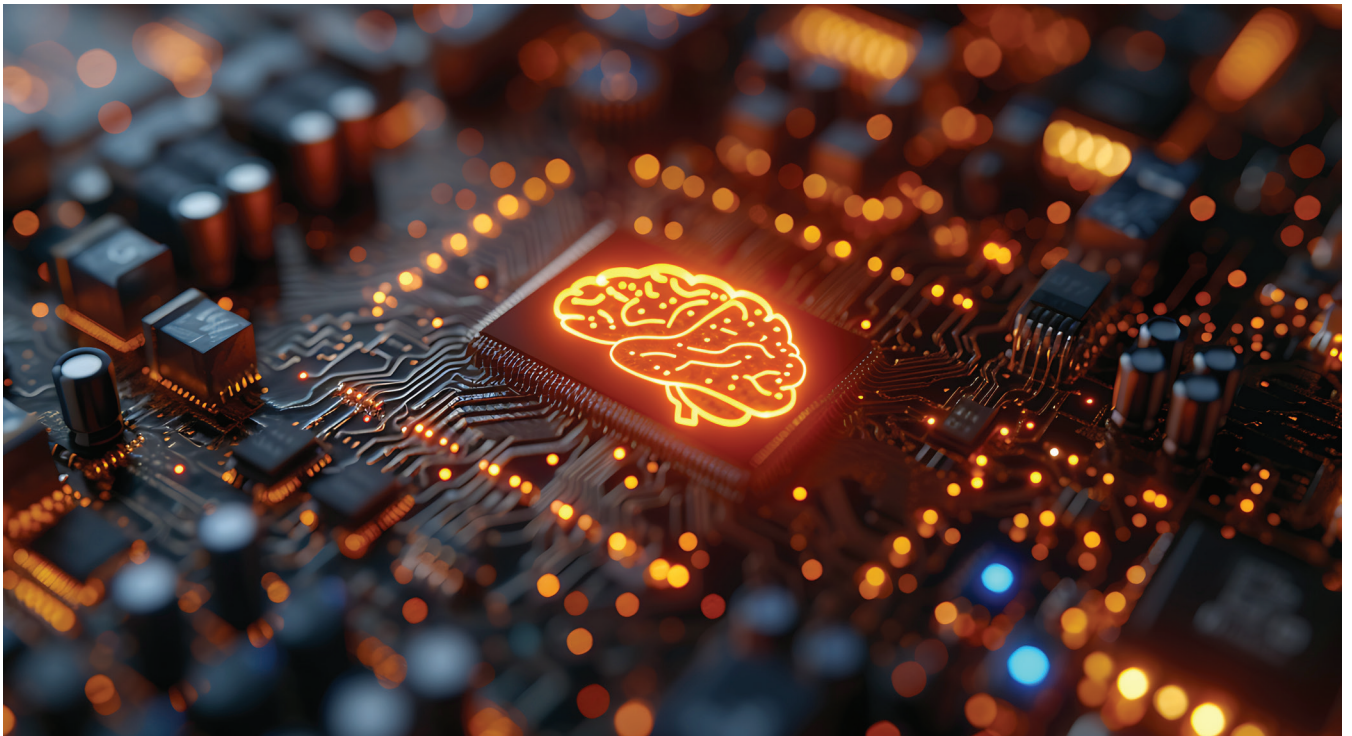
The AI-powered future of the workplace

There is no room for debate, AI is set to change the way the modern workplace operates, making resource management and organisation much easier. This means resources are booked ahead of time, employee engagement is improved, environments are personalised and no space is wasted.

However, for AI-driven systems to operate well, they need trustworthy data. Without it, chaos would reign supreme.

FURTHER READING / REFERENCE

- 1. https://en.wikipedia.org/wiki/Garbage_in,_garbage_out



Cost-Effective AI

Prioritising the full tech stack over raw compute

BY NAREK TATEVOSYAN, PRODUCT DIRECTOR AT NEBIUS AI

THE GENERATIVE AI boom is rapidly advancing technology and reshaping industries, but it's also driving an insatiable demand for computing power. Many AI start-ups are falling into the “compute trap” and focusing on gaining access to the latest, most powerful hardware regardless of cost, rather than optimizing their existing infrastructure or exploring more effective and efficient solutions to building GenAI applications.

While GPU power is undeniably critical to training large AI models and other machine learning applications, it is far from the only factor involved. Without the latest CPUs, high speed network interface cards like the InfiniBand 400 ND, DDR5 memory, and a motherboard and server rack that can tie it all together, it's impossible for top-tier GPUs like the NVIDIA H100 to perform at their full potential. Taking a broader view of compute, combined with a holistic approach to AI development – focusing on efficient data preparation, optimized training runs, and developing scalable inference infrastructure – allows for more sustainable growth of AI applications.



The limits of compute: A costly pursuit for AI start-ups

In theory, more compute and larger datasets result

in more powerful AI models. Take, Meta's Llama 3.1 8B and 405B LLMs. They were both trained using the same 15 trillion token dataset on NVIDIA H100s – but the 8B version took 1.46 million GPU hours while the significantly more powerful 405B version took 30.84 million GPU hours.

In the real world, of course, there are also practical concerns, and very few AI companies can afford to compete directly with tech giants like Meta. Instead of falling into the compute trap and trying to match the compute spend of some of the richest companies in the world, many companies would benefit from focusing on the entire tech stack driving their ML development.

While Llama 8B isn't as powerful as Llama 405B, it still outperforms many older, larger models—thanks to innovations beyond just deploying more compute. The power of integration: full-stack AI development. Managing the entire AI development lifecycle – from data preparation and labelling to model training, fine-tuning, and inference – on a single platform offers significant advantages.

Developing and deploying an AI application on a single full-stack provider means your team only has to learn a single set of tools, rather than multiple

different platforms. Keeping data on a single platform eliminates the inefficiencies of multi-cloud environments. Perhaps most usefully, if you run into any issues you are dealing with a single support team who understands the whole stack.

There are potential financial benefits too: Using a single infrastructure for data handling, training, and inference can often lead to better pricing, lowering the overall cost of your AI operations.

Exploring alternatives: Tailored platforms for AI start-ups

While major cloud providers like AWS, Microsoft Azure, and Google Cloud might seem like obvious choices, they're not always the optimum fit for AI start-ups and scale-ups.

Of all the cloud computing platforms available, the Big Three are the most expensive. If you have lots of venture funding or are a massive tech company, this might not be an issue – but for most AI companies bigger cloud providers don't offer a good ROI. Furthermore, they aren't optimised for AI specific operations, and so you are likely to pay significant premiums for features you don't need.

Dedicated full-stack AI platforms like Nebius offer a much more attractive alternative. These platforms are designed specifically for AI development, providing affordable compute and hardware setups

Using a single infrastructure for data handling, training, and inference can often lead to better pricing, lowering the overall cost of your AI operations

tailored for both training and inference. You can focus on developing, training and optimising your AI models confident that they're running on the right hardware for the job, not navigating a sprawling server backend or wondering why your expensive GPUs aren't getting the data throughput they should.

While leveraging a full-stack approach to ML development requires thought and planning, doing it at the start will minimise your ongoing infrastructure costs. A better optimised application not only reduces the cost of training runs but should also reduce the cost of inference. And these savings can compound over multiple generations of AI models. A slightly more efficient prototype can lead to a much more efficient production model, and so on into the future. The choices made now could be what gives your company the runway it needs to reach an IPO.

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

ANGEL
EVENTS



Generative AI isn't a threat but an essential co-collaborator for IT teams

Organisations are always looking for ways to enhance and improve their IT practices and processes. Whether beefing up security or ensuring their IT estate runs more efficiently, IT teams are constantly re-evaluating how they manage their systems and solutions.

BY KRISHNA SAI, SENIOR VP OF TECHNOLOGY AND ENGINEERING, SOLARWINDS

THIS MIGHT explain why some IT teams are now eyeing the potential of generative AI (GenAI) to help automate tedious tasks to save time and money. They're looking at how GenAI could support IT service management (ITSM) – the framework governing the implementation and management of IT services.

Even at this early stage, there is a growing consensus on how GenAI has the ability to enhance ITSM by automating tasks, predicting issues and improving decision-making.

GenAI is able to handle repetitive tasks, such as processing service requests, resetting passwords and updating user permissions, reducing manual workloads and freeing up IT staff to focus on more complex issues. In some cases, GenAI is also able

to use data to predict future IT service demand, helping IT teams prepare resources and adjust capacity. However, not everyone is convinced. Some more cautious IT teams are struggling to identify which business functions can truly be improved by GenAI.

GenAI makes effective ITSM accessible for organisations of any size

This should come as no surprise. Whenever a new technology is launched, there's a broad spread of reactions – from early adopters to those who prefer to 'wait and see'.

What we do know, though, is where GenAI has been adopted, it's beginning to make a real impact – especially concerning its integration into ITSM and its ability to offer affordable benefits



for businesses of all sizes. And it's an important consideration because robust ITSM solutions have traditionally been reserved for larger enterprises with the resources to invest in technology and skilled IT workers.

Now – thanks to GenAI – small and medium-sized businesses (SMBs) are able to access scalable ITSM features with no extensive financial investment or skilled workforces required. It's a technology shift that helps them automate complex ITSM functions without needing large, specialised teams.

For example, with a GenAI-enhanced ITSM solution, SMBs can benefit from advanced reporting and analytics and streamlined workflows. AI-driven analytics – capable of processing vast datasets at speed – offer detailed insights able to help lean IT teams quickly resolve issues and support decision-making.

GenAI also revolutionises workflow management at IT service desks by automating routine tasks and providing intelligent assistance. It's an approach that optimises productivity, allowing IT professionals to focus on more complex issues while delivering improved efficiency and service quality to end-users.

For instance, AI can autonomously handle incident triage, categorisation and prioritisation, helping ensure swift and accurate resolution of IT issues. What's more, it can enhance training and skill development, enabling IT teams to acquire new skills and stay updated with evolving technologies.

GenAI and human collaboration are key to powerful ITSM

While there are clear advantages to greater automation, some have expressed concern about how adopting GenAI may threaten jobs. In reality, though, GenAI in ITSM works hand-in-hand with IT professionals – not in place of them.

It's a point underscored by the recent SolarWinds IT Trends Report – AI: Friend or Foe – which found IT workers remain unconcerned about AI taking over roles. Of the nearly 700 IT staff members and leaders surveyed, 90% said they have a positive opinion of AI. They see it as a valuable tool that enhances their capabilities and helps them achieve business goals. But like any new technology, there need to be ground rules. This is why it's important to consider frameworks like AI By Design, which establishes guiding principles for optimal practices around AI.

One of those principles is 'Simplicity and Accessibility', which maintains that all human interaction with AI should be seamless and intuitive, preventing fatigue and streamlining decision-making. In other words, GenAI should be able to empower IT professionals to make better decisions – not make those decisions for them.

Human IT teams remain in charge

'Whether an advisor or a sidekick, AI doesn't have carte blanche to make decisions in isolation', said the report. 'For the sake of security, privacy, and output quality, IT leaders should welcome AI into their teams' workflows while prioritising human oversight and explainability.

Human oversight and transparency are foundations for building trust in AI and its impact—not just within IT organisations but for their colleagues and customers.'

Although there are some concerns, the truth is human oversight is a key factor in AI-driven ITSM operations. Far from being a threat to jobs, it enables IT professionals to monitor AI-enhanced tools, intervene when necessary and adjust to improve performance. This oversight helps prevent potential issues and ensures that AI tools are used responsibly and effectively.

By combining AI's processing power with human judgement, organisations can achieve a higher level of operational excellence. As a technology, GenAI excels in incident management and root-cause problem-solving.

It can quickly analyse incident patterns, identify root causes and suggest remediation steps. It's then up to IT professionals to review these suggestions, make adjustments as needed and implement solutions. This collaborative approach helps accelerate incident resolution, minimise downtime and improve overall service quality.

GenAI's integration into ITSM might seem like it's reaching a pivotal moment. But it's only the beginning. Far from being a threat, it's rapidly becoming a deeply effective way to empower IT teams.





Beyond the golden cages

Modernising testing workflows for agile network innovation

BY ALEKSI HELAKARI, HEAD OF TECHNICAL OFFICE, EMEA, SPIRENT
AND PATRICK JOHNSON, CMO, APNT - A SPIRENT PARTNER

CHANGE is difficult, but often necessary. The testing discipline sits stubbornly at the edge of that precipice. Many practitioners still need to understand that bringing out the next generation of testing technology is going to involve breaking some of the processes, tools and technologies that they're most enamored of.

This is best expressed in the notion of a “gold” test environment. These brittle arrangements are closely guarded and precisely calibrated to test products over and over again under the same conditions: One stray data point could throw the entire arduous process off. They're also becoming golden cages, obstructing the next evolution of testing. If we want to get there, we're going to have to melt some gold.



How a gold build becomes a golden cage

As I've seen time and time again through my work with APNT and Spirent, test labs generally don't react well to change. They generally rely on the “gold build” - the highly refined and delicately calibrated set of conditions and settings that test teams have to regress against.

Once a device or system is slated for release, the configuration files and test artifacts are locked in as “the gold build,” setting a baseline for future tests. This creates a brittle, delicate and static environment which is painstaking to set up and recreate.

A single gold build has to be consistent every time for the multiple cycles of testing that a given release will undergo. This is a particularly delicate set of conditions within physical testbeds. Routers have to be physically connected to the test tools, and fibre optic cables have to be carefully placed because damage to these can cause significant attenuation changes.

Given the careful set up required, test teams are rightly sensitive about other teams rearranging or upsetting their work when they need to test another product.

If an organisation has one testbed and multiple teams testing multiple products, that gold build has to be undone and the testbed has to be restructured so that other teams can use that equipment.

Suddenly the risk of manual human error gets introduced into the process again - and that gold build will have to be painstakingly rebuilt. From there, teams become ever more protective over their particular gold builds, jealously guarding their delicate configurations.

This is happening at exactly the wrong time: Demand for new technology is skyrocketing, innovation cycles are getting shorter, and pressure is mounting to release. The gold build is increasingly an artifact from a previous age, slowing testing practices when they need to accelerate and scale.

The race to release

First, let's examine how the demands around testing are changing. We're currently living in an age where companies are competing over a series of potentially transformative technologies such as 5G, AI, IoT and more.

In these races, time to market has a huge effect on market capture. Indeed, the race to release products and services around these technologies is so competitive, that the first mover attains huge advantage and later entrants have a disproportionately diminished advantage. One report by Harvard Business Review found that those that release first, generally capture about 30 to 40 percent of market share, while competitors don't even come close compared to their faster colleagues. This is especially pronounced within 5G, which is now seeing both a heated race to release and with whom many operators, struggling to automate testing capabilities. It has - thus far - soaked up huge amounts of investment and operators now want to recoup their investments quickly. Getting their offerings to market quickly will be crucially important to recoup those investments.

Mounting complexity

The technologies that are now being tested are more complex too. Whereas previous generations of technology may have required a handful of test cases to properly evaluate, technologies like 5G and AI and the products and services that stem from them require hundreds, if not thousands of tests across myriad use cases and conditions to be properly tested. That's partly about the potentially endless series of use cases that these technologies will be used for such as medical imaging or autonomous vehicles and it's partly about the bold new capabilities - such as network slicing - those technologies will come with. Ultimately, complexity of these new technologies require new levels of testing which cannot be achieved manually.

Take 5G OpenRAN, for example. This revolutionary innovation blends the hardware-based systems of classical telecoms technology, with the software based infrastructure of 5G, thus creating an "open" virtualised system. Within the myriad components and processes OpenRAN will involve, testing this technology will require the expertise of highly-

qualified and hard-to-hire personnel and thousands of test cases across the galaxy of components and technologies that OpenRAN involves.

Automation will bring agility

Testing needs to move towards agile operations. These will require dynamic, automated testing environments that can evolve alongside product development. Embracing continuous integration and adaptive testing frameworks will enable teams to test frequently, more efficiently, and at a scale that matches the speed of today's innovation. By modernising testing workflows, the industry can break free from the limitations of gold builds and usher in an era of smarter, more agile product development.

The manual holdover of the gold build has to give way to an automatable, scalable and shareable environment, virtualised and driven by software. Scaling up physical infrastructure - as would have been the solution in previous generations - is simply no longer feasible. However, by consolidating test beds and automating into a shareable - and crucially, reproducible - environment. This will allow teams to create and store an exact blueprint - that including all the precise resources, configurations and connectivity settings - that can be shared across teams. From there, that gold build blueprint can be restructured instantly, robustly and without the risk of human error.

This will ultimately allow testing teams to schedule equipment when they need it and share testing resources as required. But most importantly, it will allow test teams to scale their testing hugely while maintaining the precise testing conditions they require. This not only provides a path forward to accommodate modern testing demands but will likely result in significant cost savings as the costs of physical infrastructure are diminished and expensive, energy-hungry lab equipment can be decommissioned and replaced with more efficient solutions.

Melting the gold build

The essential problem here is that with the rapidly increasing demand, exponentially accelerating innovation cycles, market pressures and the sheer speed of technical growth, gold builds are far too brittle a tool. In shackling themselves to gold builds, organisations are inviting inefficiencies and delays. For many enterprises, that should ultimately be a question of long-term survival.

Testing workflows need to be modernised to accommodate the scale and speed of modern innovation. That can only be achieved through modernisation and a dynamic, automated test infrastructure that can embrace continuous integration and adapt to shifting demands. From there, testing technology will be able to scale at a speed that matches modern appetites for agility and innovation.



Why effective visibility in the cloud is critical: and how to get there

Many IT and Security leaders are confident they're sufficiently secure across their entire IT infrastructure, from on-premises to cloud.

BY CARY WRIGHT, VP OF PRODUCT MANAGEMENT, ENDACE

HOWEVER, the reality is that most organisations lack sufficient visibility into their on-premise network infrastructure, let alone adequate visibility into their cloud-based networks. This lack of visibility - particularly in cloud environments - is creating opportunities for attackers to breach network defences without being detected and giving them ample time to conduct reconnaissance, plan and carry out their attacks.

The stats don't lie: 45% of breaches are cloud-based (from IBM Cost of a Data Breach Report 2023.) In spite of this, companies continue to move sensitive assets to the cloud: according to the Thales 2023 Cloud Security Study, 75% of respondents report that 40% or more of their data in the cloud is sensitive (up from 49% of respondents in 2021). In the same study, 55% of respondents say it is more complex to manage data in the cloud than it is in on-premises environments.

Visibility in the cloud is a common issue. Part of the

reason why organisations lack visibility into cloud infrastructure is because both NetOps and SecOps teams have often been "late to the party" when shifting workloads to the cloud.

Organisations create cloud migration project teams but often neglect to include NetOps and SecOps teams in the initial planning. Cloud architects are also often insufficiently aware of what these teams need to do their jobs effectively.

Once the migration is completed, NetOps and SecOps teams are handed responsibility to monitor and secure the new cloud infrastructure, often without the necessary visibility and monitoring infrastructure required to do this effectively.

Layers of defence and visibility are critical, on-premise and in cloud. Skilled threat actors deploy multiple techniques to remain in stealth mode for as long as possible. Evasion techniques enable



attacks to sneak past network and endpoint security devices undetected, threat actors often cover their tracks by disabling logging, deleting evidence on the systems they attack, and sometimes executing vulnerabilities to take down security tools such as EDR, Firewalls, or NDR/IDS tools. Especially for SecOps teams, multiple layers of defence and visibility are essential to ensure teams are not defending in the dark.

Robust security requires multiple layers of visibility to ensure that we can still defend when the threat actor evades or disables one or more layers of defence. Teams defending on-premise networks typically use a variety of tools and technologies - including packet capture - to proactively monitor and secure these networks. Packet capture is extremely difficult for an attacker to evade or manipulate, threats always use the network and packet capture is usually invisible to an attacker. Packet evidence has proven invaluable to those defending on-premise networks but how can organisations obtain the same level of visibility in public cloud networks when they don't "own" the infrastructure.

Until relatively recently, full packet capture data in the public cloud simply wasn't an option, leaving teams reliant on flow monitoring and logs as the only cloud network telemetry options. This lack of access to definitive packet-level evidence meant the well-established playbooks and workflows teams have honed to protect their on-premise infrastructure, didn't translate well into cloud environments.

Thankfully, times have changed. Customers can now use VPC mirrors, virtual span ports, cloud packet brokers or virtual TAP agents, to enable full packet data in public cloud environments. This means they can now use their proven workflows and tools to protect their cloud network environments too.

Moreover, with a solution that can provide visibility into both on-premise and cloud networks from a single-pane-of-glass, teams gain visibility into network activity across the entire hybrid cloud network. This ubiquitous visibility is a huge advantage. For example, it can enable teams to track attackers that have successfully compromised public cloud infrastructure and then leverage that cloud access to extend their access to on-premise infrastructure. When visibility data is siloed across on-premise and cloud environments this is almost impossible to do - at least impossible to do quickly enough to respond to attacks and shut them down.

However, many organisations are not yet aware that full packet capture in the public cloud is possible. Indeed, many have not yet fully grasped the need for it. One often cited - and probably apocryphal - story has a CIO exclaim confidently "but there are no packets in the cloud!" Needless to say, that's not true. There are packets in the cloud. And just as with on-premise networks, packet data provides the only

truly definitive source of evidence of exactly what happens on cloud networks too.

What do NetOps and SecOps teams need for effective network visibility in the cloud?

Organisations should look to establish the same level of visibility into their public cloud network environments as they have for their on-premise and private cloud environments. Importantly, that would include having always-on packet capture to record as much full packet data as their budget allows. For many organisations this is a mandatory requirement anyway. For example, US Federal agencies are required to collect a minimum of 72 hours of full packet capture data (as per OMB M-21-31) that they can provide to CISA and/or the FBI if required for a breach investigation.

Regardless of regulatory obligations, having full packet data available to NetOps, SecOps and DevOps teams is very valuable. It saves immense amounts of time in the investigation and resolution of network security and performance issues by avoiding the need to correlate multiple telemetry sources. And it gives teams certainty. They no longer need to formulate theories about what took place on the network. The definitive evidence is right there in the packets.

Implementing "always-on" packet capture is essential. Triggered packet capture - which activates capture only in response to a trigger event - is unsafe, because it relies on being able to predict and detect events where packet data is going to be essential for investigations. Packets are most useful when investigating the most serious threats, those that are unknown and not predictable - such as with a Zero Day threat, disabled layers of defence, complex evasion, or a network failure that is out of your control. It's also important not just to record the full packet data, but also to ensure it's easy for analysts to quickly locate the packets of interest from within what may be petabytes of recorded packet data. Having the ability to quickly search for and find the packet data related to a specific event is key.



Ideally, organisations should look for a solution that integrates this capability directly into the monitoring tools that NetOps and SecOps teams are already using - so they can go directly from a detected event to the related packets as part of a seamless investigation workflow. Forcing analysts to stop in the middle of an investigation to pull down large capture files and then slice-and-dice them to locate packets of interest is slow and cumbersome. These days, it's unnecessary too as long as you select a packet capture solution that offers turnkey API integrations with your tools.

The additional benefits of ubiquitous hybrid-cloud visibility

A recent report from Enterprise Management Associates (EMA) - NetSecOps: Examining How Network and Security Teams Collaborate for a Better Digital Future - outlines the significant benefits that accrue from encouraging Network and Security teams to collaborate more closely - particularly as organisations migrate workloads to the cloud.

EMA's research highlights organisations which share visibility tools across teams see increased collaboration between security and network teams. This helps break down traditional silos and in many cases has resulted in the formation of hybrid NetSecOps teams. Organisations that encourage this closer collaboration reap significant benefits including:

- Reducing security risks (43.1%)

- Improving operational efficiency (39.8%)
- Faster resolution of network/application performance problems (39.5%)
- Faster detection and resolution of security issues (39.1%)
- Cost savings (38.5%)
- Network resilience (34.5%)
- Reduced architectural complexity (24.3%)

Collaboration between teams is also facilitating a two-way exchange of knowledge. Network teams can share their expertise in packet analysis, while security teams can provide insights into cyber threats and attack patterns. This gives team members the opportunity to broaden their skills and increases both their capability and value - further helping organisations to battle the skill shortages that the industry faces.

There are clear advantages to fostering closer collaboration between NetOps and SecOps teams – to promote the use of shared tools, workflows, and processes. As cloud adoption continues to accelerate, the ability to capture and analyse packet data across hybrid environments is now increasingly crucial. Organisations that plan for this need and architect their networks to ensure they can meet it are significantly better prepared to defend their organisations from costly outages, performance issues and cyberattack than those that realise the need too late.

DW ROUNDTABLE

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



- 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 editor, Phil also, this can include 3 speakers
- Questions prepared and shared in advance

Cost: £6995

Contact: Jackie Cannon jackie.cannon@angelbc.com

**ANGEL
EVENTS**

The top trends impacting infrastructure and operations for 2025

Gartner, Inc. has highlighted the six trends that will have a significant impact on infrastructure and operations (I&O) for 2025. Gartner analysts presented the findings during the recent Gartner IT Infrastructure, Operations & Cloud Strategies Conference.

“THESE TRENDS give the opportunity for I&O leaders to identify future skills requirements and seek insights to help meet implementation requirements,” said Jeffrey Hewitt, Vice President Analyst at Gartner. “They will provide the differentiation needed for enterprises to gain the optimal benefits from their I&O operations in 2025.”

Trend No. 1: Revirtualization/devirtualization

The recent license changes for certain vendor-based solutions have forced many I&O teams to re-evaluate their virtualization choices with some moving more to public cloud, some turning to distributed cloud and some moving to private cloud. This involves multiple options beyond just changing hypervisors.

“I&O leaders must inventory all current virtualization implementations and any related interdependencies,” said Hewitt. “Evaluate alternative paths including hypervisors, hyperconvergence, distributed cloud, containerization, private cloud and devirtualization. Identify existing I&O skills and how those need to evolve to support top choices.”

Trend No. 2: Security Behavior and Culture Programs

As the sophistication and variety of attacks increases, security programs must evolve to address behavior and culture to optimize their effectiveness. Security behavior and culture programs (SBCPs) are enterprise-wide approaches to minimize cybersecurity incidents associated with employee behavior.

SBCP programs result in improved employee adoption of security controls and reductions in behavior not considered secure. They enable I&O to help support the more effective use of cybersecurity resources by employees.

Trend No. 3: Cyberstorage

Cyberstorage solutions utilize a data harbor made up of data that is fragmented and distributed across multiple storage locations. The fragmented data can be instantly reassembled for use when needed. Cyberstorage can be a dedicated solution with comprehensive features, a platform-native service offering with integrated solutions, or a collection of stand-alone products that augment storage vendors with cyberprotection capabilities.

“For cyberstorage to be successful, I&O leaders should identify the risks of costly and disruptive storage threats, combined with increasing regulatory and insurance expenses to build a business case for cyberstorage adoption,” said Hewitt.

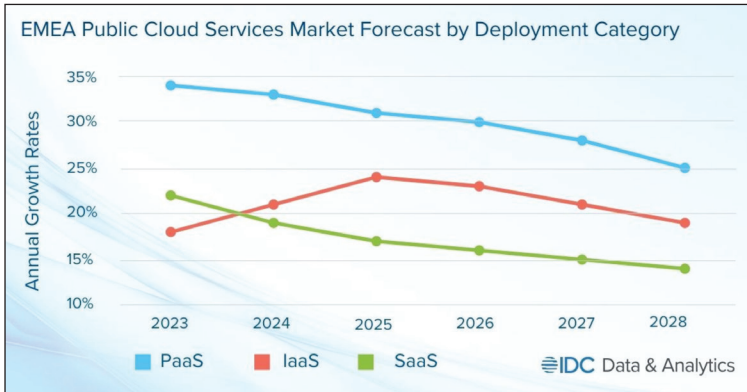
Trend No. 4: Liquid-cooled Infrastructure

Liquid-cooled infrastructure consists of rear-door heat exchange, immersion and direct-to-chip. It enables I&O to support new chip generations, density and AI requirements, while also providing I&O opportunities to flexibly place infrastructure to support edge use cases.

“Liquid cooling has evolved to move from cooling the broader data center environment to getting closer and even within the infrastructure,” said Hewitt. “Liquid-cooled infrastructure remains niche

➤ Figure 1:
Gartner Top
I&O Trends
for 2025.
Source: Gartner
(December
2024)





Source: IDC's Worldwide Semiannual Public Cloud Services Tracker, November 2024

today in terms of use cases but will become more predominant as next generations of GPUs and CPUs increase in power consumption and heat production.”

Trend No. 5: Intelligent Applications

Generative AI has revealed applications’ potential to operate intelligently, which has created the expectation for intelligent applications. Intelligent applications adapt to their user’s context and intent, thereby reducing digital friction. It can interoperate in pursuit of their own, as well as their users’ intents, by marshaling the appropriate interfaces to external APIs and connected data.

Ultimately, intelligent applications reduce required intervention and interactions on the part of I&O. It also optimizes processes and utilization while reducing resource overhead.

Trend No. 6: Optimal Infrastructure

Optimal infrastructure is when I&O teams place a highly significant emphasis on the best infrastructure choices for a given use case across a range of deployment styles. This approach utilizes a business-based focus so that executives outside of IT can understand why infrastructure choices are made from their perspectives.

“These choices are ultimately aligned with platform engineering adoption,” said Hewitt. “They allow I&O to align infrastructure choices with the business objectives of the overall organization. They also facilitate the support and approval of business unit leaders and C-level executives.”

EMEA Public Cloud Services market poised for rapid growth

The Europe, Middle East, and Africa (EMEA) public cloud services (PCS) market, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), is projected to generate \$203.0 billion in revenue for 2024. That’s according to the latest Worldwide Semiannual Public Cloud Services Tracker from International Data Corporation (IDC), which forecasts that the EMEA PCS market will reach \$415.1 billion in 2028, representing a compound annual growth rate (CAGR) of 20.0% for the 2023–2028 period.

SaaS, encompassing both SaaS – Applications and SaaS – System Infrastructure Software (SIS), continues to be the largest cloud deployment category, and is projected to make up 64.4% of the total PCS market in 2024.

Due to its size and maturity, SaaS is experiencing the slowest rate of growth among the different cloud deployment models. In contrast, PaaS is the fastest-growing segment, with a projected CAGR of 29.3% for 2023–2028 forecast period, followed by IaaS with a CAGR of 21.6%.

The increased adoption of AI, particularly generative AI (GenAI), combined with ongoing investments in cloud datacenters by global cloud service providers across EMEA, is driving the overall demand for public cloud services. Both end users and technology providers are investing in AI-ready infrastructures and platforms. Global tech companies will continue to invest in GenAI, embedding more features and functionalities into their existing portfolios. This will create additional opportunities for growth in the IaaS and PaaS markets, boosting adoption of such services across the EMEA region.

“As enterprises adopt GenAI to gain a competitive advantage, the need for scalable, on-demand infrastructure continues to rise,” says Manish Ranjan, research director for software and cloud at IDC EMEA. “High-performing compute resources, such as GPUs and other accelerated computing, are essential for running AI/GenAI workloads.

Public cloud service providers are becoming the primary entry point, offering the necessary infrastructure to support GenAI initiatives without significant up-front investments.”

From a sub-regional perspective, Western Europe dominates the EMEA market, accounting for over 80% of its revenue, followed by the Middle East and Africa (MEA) and Central and Eastern Europe (CEE). Germany, the U.K., France, and Italy remain the key destinations for cloud investments.

However, global hyperscalers like Google, AWS, Microsoft, and Oracle are aggressively expanding their cloud regions in Finland, Greece, Denmark, the Netherlands, Belgium, Austria, and Spain, boosting cloud adoption across Europe. Similarly, MEA, the fastest-growing sub-region for IaaS, is a hotspot for global cloud providers, with AWS, Microsoft, Google, Oracle, and Alibaba establishing cloud regions in Saudi Arabia, the UAE, South Africa, Qatar, and Bahrain, and planning expansions in Kuwait, Morocco, Kenya, and other tier 2 markets.

AI spending to surpass \$100 billion in next five years

The global Artificial Intelligence (AI) infrastructure market is on track for unprecedented growth, poised to surpass \$100 billion USD in spending by 2028, according to the latest findings from the

Storage spending in AI infrastructure has been driven by the need to manage large datasets required for training AI models, as well as storage of training, checkpoints and repositories of data for inference phases. This category reported a 36% year-over-year growth rate in 1H24 with 56% of the spending coming from cloud deployments

International Data Corporation (IDC) Worldwide Semiannual Artificial Intelligence Infrastructure Tracker. Organizations increased spending on compute and storage hardware infrastructure for AI deployments by 37% year-over-year in the first half of 2024, reaching \$31.8 billion.

The AI infrastructure market has sustained double-digit growth for nine consecutive half-years, driven primarily by investment in servers for AI deployments. In 1H24, servers accounted for 89% of the total spending, growing 37% compared to the same period last year.

AI Infrastructure deployed in cloud and shared environments accounts for 65% of the total server spending in AI in 1H24, as hyperscalers, cloud service providers and digital service providers expand their infrastructure capabilities. Traditional enterprises, by contrast, have largely lagged behind in adopting on-premises AI infrastructure.

Servers with an embedded accelerator are the preferred infrastructure for AI platforms accounting for 58% of the total server AI infrastructure spending -- growing 63% in the first half of the year 2024. IDC projects that accelerated servers will exceed 60% of the server AI infrastructure spending by 2028, growing at a 19% 5-year CAGR rate.

Storage spending in AI infrastructure has been driven by the need to manage large datasets required for training AI models, as well as storage of training, checkpoints and repositories of data for inference phases.

This category reported a 36% year-over-year growth rate in 1H24 with 56% of the spending coming from cloud deployments. The United States leads the global AI infrastructure market, accounting for almost half of the total spending in 1H24, followed by PRC (23%), APJ (16%), and EMEA (10%).

Over the next five years, IDC expects the APJ region to grow at the fastest CAGR (20%) followed by the USA (16%), EMEA (13%) and PRC (11%). By 2028, IDC forecast AI Infrastructure spending to reach \$107Bn with servers deployed in cloud environments at 75% of the market total and accelerated servers around 56% of the total market spending.

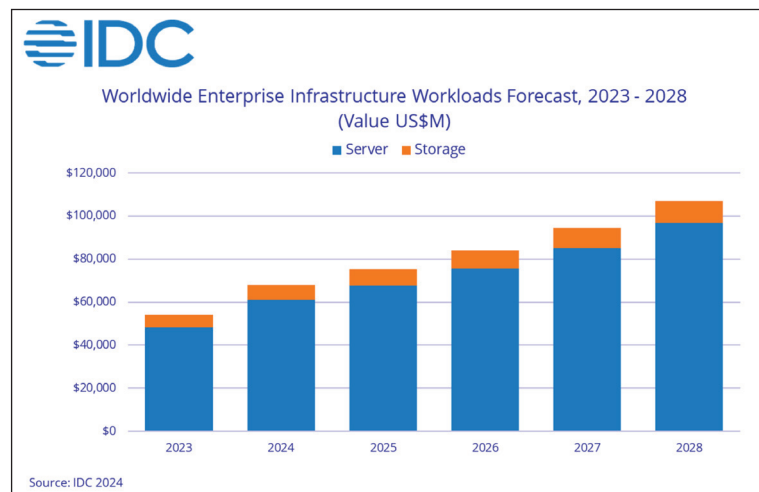
"IDC expects AI adoption to continue growing at a remarkable pace as hyperscalers, CSPs, private companies, and governments around the world are increasingly prioritizing AI. Growing concerns around energy consumption for AI infrastructure will become a factor in datacenters looking for alternatives to optimize their architectures and minimize energy use" said Lidice Fernandez, Group Vice President, Worldwide Enterprise Infrastructure Trackers.

30% of Fortune 500 companies will offer service through only a single, AI-enabled channel by 2028

By 2028, 30% of Fortune 500 companies will offer service only through a single, AI-enabled channel that allows communication through text, image and sound, according to Gartner, Inc.

Multichannel service journeys have become increasingly complex and expensive, leading to a disjointed customer experience and reduced customer retention. Service and support leaders will reexamine omnichannel strategies and leverage advancements in voice-enabled conversational AI to dramatically simplify the service experience.

Instead of offering multiple, distinct channels, a single, AI-powered channel with uninterrupted transitions between different modes of interacting - for example voice, chat, and video - will exist even within the same interaction.



“As GenAI continues to mature and facilitate seamless voice interactions, voice-based customer service isn’t going away. It will instead evolve to meet customers’ needs for a more simple service experience,” said Patrick Quinlan, Senior Director Analyst, in the Gartner Customer Service and Support practice. “Service and support leaders must pivot from a long-held focus on which channels customers use, to a focus on how customers want to communicate.”

Other Gartner predictions to help service and support leaders respond to the changing landscape in 2025 and beyond include:

Seventy percent of customer service journeys will begin – and be resolved – in conversational, third-party assistants built into their mobile devices by 2028.

GenAI has changed the way consumers search for and understand information. In fact, a Gartner survey of 5,459 respondents in August and September 2024 revealed that 45% of customers report using GenAI in their personal life, at work, or both.

With conversational GenAI so firmly integrated into the mobile device experience, customers will self-solve through third-party assistants such as Apple AI and Google Gemini rather than resolve issues through a service organization’s official channel.

“Official customer service channels are higher-effort and more complicated, and customers will be drawn to third-party AI platforms that offer quick fixes and more seamless navigation,” said Quinlan.

“If a customer can simply ask their phone for the answer, organizations will need to evaluate if their investments in self-service portals are paying off and consider possible customer-facing conversational AI solutions.”

By 2027, service organizations will see a 300% increase in fraud attempts over 2023 levels.

Conversational AI tools will appeal to fraudsters who will utilize the same technology to bypass automated systems and deceive live service agents.

To combat this, Gartner expects service and support organizations will develop strategies to counter fraud and protect customers, implementing sophisticated identity verification and multi-layered security requirements for the simplest of interactions.

“It’s important to note that though the intention was to reduce customer effort, a single, AI-enabled channel may actually increase efforts and lead to customer churn,” said Quinlan. “Leaders will need to balance strategies to reduce effort with those to protect customers from fraud.”



DIGITALISATION WORLD

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

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

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



REGISTER TO ATTEND



The Largest Data Centre Event in the World

Shape the future of **data centres** on **12-13 March 2025**. Tackle AI's impact, sustainability challenges, and global regulations head-on. Discover cutting-edge solutions and bridge the skills gap. Join the world's largest data centre gathering to drive innovation in our rapidly evolving industry.

www.datacentreworld.com/digitalisationworld

DATA CENTRE WORLD

12-13 March 2025 Excel London
www.datacentreworld.com

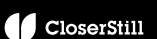
INCORPORATING



ACCREDITATIONS



ORGANISED BY



TECH SHOW
LONDON
techshowlondon.co.uk

THE MOST IMPORTANT TECHNOLOGY EVENT FOR BUSINESS IN THE UK