



DIGITALISATION WORLD

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

ISSUE III 2025

 AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

[DIGITALISATIONWORLD.COM](https://digitalisationworld.com)

Is your Data centre ready for the growth of AI?

Partner with Schneider Electric for your AI-Ready Data Centres. Our solution covers grid to chip and chip to chiller infrastructure, monitoring and management software, and services for optimisation.



Keep IT cool in the era of AI

EcoStruxure IT Design CFD by Schneider Electric helps you design efficient, optimally-cooled data centers

Optimizing cooling and energy consumption requires an understanding of airflow patterns in the data center whitespace, which can only be predicted by and visualized with the science of computational fluid dynamics (CFD).

Now, for the first time, the technology Schneider Electric uses to design robust and efficient data centers is available to everyone.

- Physics-based predictive analyses
- Follows ASHRAE guidelines for data center modeling
- Designed for any skill level, from salespeople to consulting engineers
- Browser-based technology, with no special hardware requirements
- High-accuracy analyses delivered in seconds or minutes, not hours
- Supported by 20+ years of research and dozens of patents and technical publications

Equipment Models – Easily choose from a range of data center equipment models from racks, to coolers, to floor tiles.

IT Airflow Effectiveness and Cooler Airflow Efficiency – Industry-leading metrics guide you to optimize airflow.

Cooling Analysis Report – Generate a comprehensive report of your data center with one click.

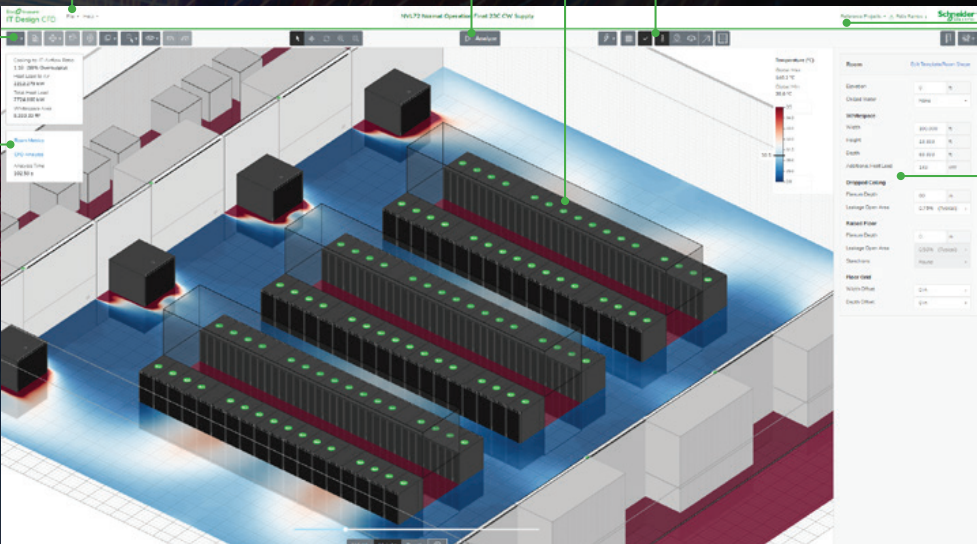
CFD Analysis – The fastest full-physics solver in the industry delivering results in seconds or minutes, not hours.

Cooling Check – At-a-glance performance of all IT racks and coolers.

Visualization Planes and Streamlines – Visualize airflow patterns, temperatures and more.

Reference Designs – Quickly start your design from pre-built templates.

Room and Equipment Attributes – Intuitive settings for key room and equipment properties.



Explore

www.se.com/uk

Staying secure in an uncertain world

THE RECENT POWER OUTAGE at Heathrow Airport is a timely reminder for businesses of all shapes and sizes to ensure that they are as well-equipped as possible to meet adversity. Sounds simple enough?

Ah, but how easy is it to understand all of the likely external and internal threats to your organisation, before making any decisions as to the necessary mitigation measures?

Power, or lack of it, is a good place to start. What would be the impact of a power outage lasting several hours on your business – everything from the relatively minor irritation of maybe losing unsaved work as IT devices shutdown to the rather more problematic scenario of being unable to communicate with suppliers and customers – and maybe your e-commerce website being offline?

In terms of being prepared for such an outage, the cost of mitigation will be a major factor – as with all insurance, there's the balance between what might go wrong and the financial impact of this versus paying high premiums 'just in case'.

Once plans have been put in place then, test, test, test. You don't want to discover that your disaster recovery/business continuity plan doesn't work in a real emergency... In our increasingly febrile world, supply chains are another area where planning for disruption makes complete sense. Whether your supplies might be hit by tariffs, however unlikely, or your existing supplier either shuts up shop, or cannot guarantee security of supply, it might be worth having a Plan B and maybe a Plan C to ensure that supply

chain disruptions are kept to a minimum.

Cybersecurity needs no introduction – but how many companies can be truly confident that their cyber defences are truly robust and, as above with a power outage, they are prepared for some kind of security breach, having a BC/DR plan in place – one which has been tested.

With employees working in many locations, on many digital devices, requiring different levels of permissions – and with the unlikely, but not impossible, scenario whereby they will get things wrong and enable a security breach, how can you minimise disruption to your business. And then there may be rogue employees who have security clearance, but are determined to cause mayhem.

And then there's the physical location of your business. With climate volatility seemingly here to stay, it's worth ensuring that your premises are not vulnerable to an extreme weather event or, if it might be, what's the plan?

These are just some of the more obvious areas on which to focus when it comes to risk assessment, but it's worth taking the time to sit down with a small team who can go through every aspect of your business and understand where the risks lie, how they can be addressed and, most importantly, deciding on the cost of disruption versus the cost of mitigation.

There are no easy answers, and no guarantee of complete resilience, but these are not reasons to ignore making some potentially crucial decisions.





24 Assessing cloud security strategies: reactive, proactive, or responsive?

As the cloud security market grows, so do the opportunities and attackers' tactics and techniques, which are becoming increasingly sophisticated, relentless, and fast

14 BPA or RPA? Maybe you need both

Comparing BPA and RPA, when to use them, and when they work well together to bring about business change

16 BPA or RPA? Maybe you need both

The cost for security breaches continues to rise. According to IBM's Cost of a Data Breach Report for 2024, the average cost for a breach was \$4.88 million, a rise of 10 percent year on year

20 What does risk mean to you?

However mature you are as an organisation around security, there are always improvements that can be made



33

22 AI, data and software: a new era of automotive safety

Imagine a world where the fear of road accidents is a distant memory

28 How the Vulnerability Operations Centre serves as an essential mission control for vulnerabilities

The vulnerability management 'to do' list can feel like a perpetual loop

30 How can businesses avoid cybersecurity blind spots in 2025?

Cybersecurity incidents in 2024 reinforced a hard truth: most breaches stem from preventable security failures rather than sophisticated attacks

33 Hybrid Multicloud as an operating model: streamlining enterprise IT

Whether scaling to meet demand, controlling costs, or boosting operational resilience, hybrid multicloud can provide the agility and control modern enterprises require.

35 How evolving businesses can overcome the AI adoption paradox

Artificial Intelligence (AI) stands as one of the most transformative technologies of our era, yet adopting its effectively presents a unique challenge

38 The hidden costs of legacy systems: Why mid-market supply chains need modernising in 2025 and beyond

Mid-market supply chain companies around the world lack the resources required to thrive and adapt in today's fast-paced digital world

40 Why are companies leaving the cloud?

Having dominated the infrastructure world for the past decade, and pulling in record profits, the undisputed reign of hyperscale cloud is coming into question

42 Worldwide security spending to increase by 12.2%

According to the latest forecast from the International Data Corporation (IDC) Worldwide Security Spending Guide, global security spending is expected to grow by 12.2% year on year in 2025



NEWS

06 Global trust in digital services declines

07 Global survey explores networking needs for AI era

08 Current state of workplace IT impedes AI productivity benefits

09 Generative and agentic AI set to transform customer service

10 Talent shortage concerns drive shift to skills-based strategies

11 IT professionals suffering from burnout

12 Companies that use IT cost optimisation to fuel innovation see improved return on investment



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

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)

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

Global trust in digital services declines

Thales 2025 Digital Trust Index reveals most industries experienced a decline in consumer trust compared to last year.

THALES has published the findings of its 2025 Digital Trust Index – Consumer Edition, revealing a universal decline in trust for digital services compared to this time last year. Across 13 different sectors, only insurance, banking and Government saw either their trust level remain unchanged or increase very slightly. When asked which sector they trusted with their personal data, not one sector reached above 50% approval. Thales surveyed over 14,000 consumers across 14 countries about their online relationship with brands and services, their privacy expectations, and how brands can earn their trust.

This decline in trust comes as nearly one in five (19%) have been informed that their personal data has been compromised in the past year. Consequently, 82% have abandoned a brand in the past 12 months due to concerns about how their personal data was being used.

Global Trust Index ranking

Banking emerged as the most trusted sector for the second year in a row. However, the research found a stark demographic shift, peaking at 51% of over 55s, and languishing at just 32% of Gen Z consumers (16-14-year-olds). Government organisations are the only sector where trust increased compared to the previous year, with 42% of global citizens ranking them as a top trusted sector with their personal data, compared to 37% last year.

News media organisations polled the lowest, with only 3% of citizens ranking them as a top trusted sector. Social media, logistics, and automotive sectors only ranked marginally higher, at 4% each.

Commenting on the findings, Sebastien Cano, Senior Vice President, Cybersecurity Products at Thales said: “Global trust in digital services is decreasing or remaining stagnant at best, even among highly regulated



industries. One area that does not remain stagnant is the threat landscape. Consumers are more aware than ever before of online threats, and the consequences of their data falling into the wrong hands. As cyber threats evolve so does consumer scepticism, and brands must continuously adapt their security measures to stay ahead and rebuild confidence.”

Too much onus on consumers

More than four in five (86%) of consumers expect some level of data privacy rights from the companies they interact with online. However, amidst growing concerns about data privacy, 63% believe that too much onus is placed on the consumer when it comes to data protection. Over a third (37%) said that they only shared their personal data with an organisation because it was the only way to access a product or service. Only 34% said it was because they trusted organisations to use this data sensibly.

This frustration is also evident when it comes to customer experience. Whether it's being kicked out of an online queue, being presented with price fluctuations, or experiencing

downtime on a website, one in three consumers (33%) voiced frustration with ecommerce, directly caused by bad bots manipulating the customer purchasing process.

Despite this growing scepticism, customers have been clear about their expectations. 64% of consumers said that their confidence in a brand or service would significantly increase if it adopted and implemented emerging or advanced technologies such as passwordless authentication, biometrics, multifactor authentication, and responsible use of AI.

“The Thales Digital Trust Index findings should be alarming to enterprises that conduct business online. The global decrease in digital trust is not only quantifiable, but preventable. Deploying modern Customer Identity Access Management (CIAM), Fraud Reduction Intelligence Platforms (FRIP), GenAI, and data privacy protection solutions properly, with optimizing the customer journey as the primary design principle, will lead to better business and consumer outcomes,” said John Tolbert, Director of Cybersecurity Research at KuppingerCole Analysts.

Global survey explores networking needs for AI era

Data centre experts predict at least 6X increase in DCI bandwidth demand over next five years, with 43% of new data centre facilities expected to be dedicated to AI workloads.

THE RAPID GROWTH of AI workloads is driving a major transformation in data center network infrastructure, with global data center experts anticipating a significant increase in interconnect bandwidth needs over the next five years, according to a study commissioned by Ciena.

The survey, conducted in partnership with Censuswide, queried more than 1,300 data center decision makers across 13 countries. More than half (53%) of respondents believe AI workloads will place the biggest demand on data center interconnect (DCI) infrastructure over the next 2-3 years, surpassing cloud computing (51%) and big data analytics (44%). To meet surging AI demands, 43% of new data center facilities are expected to be dedicated to AI workloads. With AI model training and inference requiring unprecedented data movement, data center experts predict a massive leap in bandwidth needs. In addition, when asked about the needed performance of fiber optic capacity for DCI, 87% of participants believe they will need 800 Gb/s or higher per wavelength.

“AI workloads are reshaping the entire data center landscape, from infrastructure builds to bandwidth demand,” said Jürgen Hatheier, Chief Technology Officer, International, Ciena. “Historically, network traffic has grown at a rate of 20-30% per year. AI is set to accelerate this growth significantly, meaning operators are rethinking their architectures and planning for how they can meet this demand sustainably.”

Creating more sustainable AI-driven networks

Survey respondents confirm there is a growing opportunity for pluggable optics to support bandwidth demands and address power and space challenges. According to the survey, 98% of data center experts believe pluggable optics are important for



reducing power consumption and the physical footprint of their network infrastructure.

Distributed computing

The survey found that, as requirements for AI compute continue to increase, the training of Large Language Models (LLMs) will become more distributed across different AI data centers. According to the survey, 81% of respondents believe LLM training will take place over some level of distributed data center facilities, which will require DCI solutions to be connected to each other. When asked about the key factors shaping where AI inference will be deployed, the respondents ranked the following priorities:

- AI resource utilization over time is the top priority (63%)

- Reducing latency by placing inference compute closer to users at the edge (56%)
- Data sovereignty requirements (54%)
- Offering strategic locations for key customers (54%)

Rather than deploying dark fiber, the majority (67%) of respondents expect to use Managed Optical Fiber Networks (MOFN), which utilize carrier-operated high-capacity networks for long-haul data center connectivity.

“The AI revolution is not just about compute—it’s about connectivity,” added Hatheier. “Without the right network foundation, AI’s full potential can’t be realized. Operators must ensure their DCI infrastructure is ready for a future where AI-driven traffic dominates.”

Current state of workplace IT impedes AI productivity benefits

Workplace research finds employee productivity a top priority, though current systems sorely lacking.

A NEW Lenovo global survey of 600 IT leaders reveals that while 79% of respondents believe AI will allow employees to focus on more impactful work, less than half feel their current digital workplace solutions adequately support productivity, engagement, and innovation. Only 36% believe their systems support employee engagement “very effectively” -- while a staggering 89% say organizations must first overhaul their digital workplace to fully unlock AI’s potential.

Reinventing Workplace Productivity explores the opportunities and challenges that Generative AI presents for the future of work, highlighting the urgent need for digital workplace transformation to ensure its successful adoption.

Unlocking AI’s potential for greater productivity and engagement

The report highlights that Generative AI will be a game-changer for collaboration, creativity, and productivity, outlining several key areas where AI can positively impact organizations:

- **Enhanced Collaboration:** AI-powered tools such as virtual co-authoring and real-time translations break down barriers, enabling seamless teamwork across geographies and languages.
- **Creative Empowerment:** By automating repetitive tasks, AI frees employees to focus on more strategic and innovative work, driving creative problem-solving.
- **Productivity Boosts:** AI-driven insights streamline workflows, improve efficiency, and accelerate day-to-day operations.

Nearly half (49%) of IT leaders surveyed say that creating a productive and engaging employee experience (EX) is



their top priority for the year ahead. This echoes IDC research commissioned and published by Lenovo last month – its global 2025 CIO Playbook, It’s Time for AI-nomics, found that improving employee productivity is this year’s top business priority.

Roadblocks: Personalization and adoption barriers

Despite the urgent need to transform the digital workplace around AI, several key challenges remain in its widespread adoption:

- **Personalization Gaps:** While 63% of IT leaders surveyed agree that a highly personalized digital workplace is essential, a lack of configurable devices and applications remains a top barrier. This one-size-fits-all approach leaves employees underserved.
- **Support Automation:** 61% of IT leaders acknowledge the need for AI-driven IT support automation, but many organizations still struggle to integrate these systems effectively.

Lenovo’s vision for an AI-driven future

Entering a new era of Gen AI-powered personalization, employees need to be able to think, create, and collaborate without disruption. Today’s digital workplace needs to provide hyper-personalized settings catering to the diversity of working styles, enabling companies to make the best use of their talent, while bolstering productivity.

This is not just about devices and software, the IT support that employees rely on should also be tailored to their specific requirements and abilities. To fully leverage AI’s potential, Lenovo advocates embedding generative AI into core business operations as part of a broader digital workplace transformation strategy.

“Transforming your workplace is essential to using AI effectively. Simply automating existing workflows will only yield incremental benefits.

AI changes the rules of productivity, but to realize its potential, IT leaders must work alongside their executive teams to rethink how AI can augment their organization’s value-creation levers and competitive differentiation,” said Rakshit Ghura, VP and General Manager of Digital Workplace Solutions, Lenovo. “AI must be seamlessly integrated into core operations, creating a personalized and efficient digital workplace that enhances the employee experience and drives long-term productivity.”

Core recommendations

The report provides three recommendations for businesses looking to harness AI in the workplace:

- **Simplify and personalize the employee experience:** Tailor tools, workflows, and experiences to individual roles, ensuring maximum productivity and innovation.
- **Automate IT processes:** Use Gen AI to efficiently manage devices and meet diverse employee needs, freeing up resources for higher-value tasks.
- **Transform workflows for value creation:** Rethink existing workflows and processes to fully capitalize on Gen AI’s capabilities and drive innovation.

Generative and agentic AI set to transform customer service

With less than half of consumers happy with the service they receive and only 16% of agents satisfied with their roles, AI-led transformation can unlock significant commercial potential; but customers still want a 'human factor'.

ALTHOUGH most consumers say customer service is pivotal in shaping their perception of a brand, less than half (45%) express overall satisfaction with the service they receive. This discrepancy highlights a significant opportunity for brands to enhance their customer service and foster greater loyalty.

The Capgemini Research Institute's latest report, 'Unleashing the value of customer service: The transformative impact of Gen AI and Agentic AI', finds that generative AI (gen AI) and agentic AI are emerging as key tools for organizations to make a transformative shift, elevating customer service to a strategic value driver.

However, whilst virtual agents are favored for their speed and convenience, consumers overwhelmingly prefer human agents for their empathy and creative problem-solving skills. This indicates that the future of customer service will require a strategic blend of human and virtual agents, enhanced by gen AI and agentic AI.

Customer service remains one of the most powerful tools for driving purchases, encouraging loyalty, and shaping brand perception. In fact, according to the report, almost 60% of consumers view customer service as extremely important in shaping their perception of a brand. However, there's a need to overhaul the function as both consumers and customer service agents are currently dissatisfied, with only 16% of agents reporting overall satisfaction with their roles, and a majority (65%) of executives admitting low operational efficiencies.

"With over half of consumers prepared to leave a brand due to poor customer

service, even if their purchase is good, business leaders now recognize that exceptional customer service is no longer a luxury but a strategic imperative," said Franck Greverie, Chief Portfolio & Technology Officer and Group Executive Board Member at Capgemini.

"Organizations are navigating multiple headwinds, including a lack of call center agent engagement, poor coordination between departments, and outdated legacy systems. Reimagining customer service with gen AI requires businesses to transform their digital solutions, operating model and data foundations; leaders who embrace this change will not only enhance customer satisfaction and operational efficiency but also unlock commercial opportunities for competitive edge in the market."

Most organizations have implemented or are exploring gen AI and it's already a gamechanger

According to the research, 86% of organizations have already implemented gen AI, initiated pilots, or started exploring its potential in their customer service functions.

The report states that this transformative technology will be key to overcoming multiple challenges, including addressing key customer pain points, improving agent experience and enhancing operational inefficiencies.

Notably, most consumers place a high priority on effective and speedy issue resolution, yet a significant number feel they do not regularly receive it. Prompt responses are also important but often lacking.

Among the organizations using gen AI, almost 9 in 10 are either already seeing

improved first contact resolution rates or expecting to see this benefit in the future. Similarly, most (89%) are seeing or expecting faster response times, as well as benefiting from or expecting higher agent productivity (85%), and similar proportions are experiencing or anticipating reduced operating costs.

Together, human and virtual agents could provide a seamless blend of empathy and efficiency

According to the report, most consumers (71%) feel that chatbots have improved in quality over the past 1–2 years. With the rapid acceleration of gen AI, there are notable advancements in understanding context, human emotion, and responding with empathy.

Whilst chatbots are valued for speed and convenience, over 70% of consumers prefer human agents for empathy and creative problem-solving. However, this preference varies by age, with younger consumers showing greater inclination towards chatbots and older consumers preferring human agents. Consequently, the traditional customer service function is expected to evolve into a CX center, operated by hybrid teams of human and AI agents. Less than half of organizations are fully prepared for AI-powered customer service

Despite its strategic importance, only 49% of organizations consider themselves prepared for offering AI/gen AI-powered customer service, indicating the need for a critical shift in operating model, transformation of digital solutions and uplift of their data foundation.

Without these building blocks in place, organizations could fail to fully leverage AI as a key transformation lever concludes the report.

Talent shortage concerns drive shift to skills-based strategies

Workday has released “The Global State of Skills”, revealing a pressing challenge for businesses worldwide: More than half (51%) of business leaders are worried about future talent shortages, and only 32% are confident their organisation has the skills needed for long-term success.

As AI transforms industries, the skills required to thrive in the workforce are evolving fast. However, many organisations lack visibility into the existing capabilities of their people – only 54% of leaders say they have a clear view of the skills within their workforce today.

This growing uncertainty is exposing the limitations of traditional talent management approaches that focus on job titles, degrees, and previous companies worked for. In response, organisations are accelerating a shift to skills-based talent strategies, which prioritise an individual’s capabilities over traditional credentials and provide a more agile, data-driven approach to hiring, developing, and deploying talent.

Key Findings:

- Skills-based strategies are no longer a “future of work” concept – they’re a competitive advantage. 81% of leaders agree that adopting a skills-based approach drives economic growth by improving productivity, innovation, and organisational agility.
- The movement is already underway. More than half (55%) of organisations worldwide have begun the transition to a skills-based talent model, with an additional 23% planning to start this year.
- Beyond business impact, skills-based strategies can help close opportunity gaps. Leaders cite increased access to job opportunities for employees (82%), higher workforce equity (72%), and lower unemployment (61%) as key benefits.

AI boosts the shift to skills-based talent management

AI is both a catalyst for and an enabler of this shift. While the rise of AI is transforming jobs, it is also helping

organisations build more agile, skills-driven workforces. According to the research, AI is playing a pivotal role in the transition by:

- Streamlining routine and repetitive tasks (52% of leaders agree)
- Enhancing decision making with data-driven insights (52% of leaders agree)
- Personalising learning and development programmes (47% of leaders agree)
- Predicting future skills needs (45% of leaders agree)

“At Ferring, we are committed to a culture of continuous learning where employees can connect with new skills, opportunities and projects that align with their ambitions,” said Lynn Van Oossanen, Global Head of People Solutions, Ferring Pharmaceuticals. “With AI-powered technology, we can now identify skills gaps in real-time, enabling employees to seek out growth opportunities while helping managers connect with the right talent more effectively.”

AI is accelerating, but human skills remain irreplaceable

While technical skill sets are in high demand, today’s research highlights an equally critical need for uniquely human skill sets. Social skills like communication and teamwork, and individual skills like resilience and creativity are listed as the most impactful skill gaps in organisations today, followed by digital fluency, including AI and software proficiency.

This aligns with findings from Workday’s “Elevating Human Potential: The AI Skills Revolution” report, which found that relationship-building, empathy, conflict resolution and ethical decision-making are critical for success in an AI-driven economy.

“AI is reshaping the workplace, but the human element has never been more essential,” said Chris Ernst, Chief Learning Officer, Workday.

“Organisations that embrace a skills-first mindset will not only unlock AI’s potential but also harness human ingenuity in new and transformative ways.”

Challenges to adoption – and the path forward

Despite the momentum behind skills-based strategies, business leaders cite several key challenges:

- The time required to reskill employees (43%)
- Resistance to change (38%)
- Lack of infrastructure to support skills-based talent management (28%)
- Inadequate skills measurement tools (28%)

Technology alone isn’t the solution, the research finds. Overcoming these challenges requires a shift in mindset – one that includes clear communication of the benefits (48%) and effective change management (48%) to drive adoption across organisations.

the future of talent is skills-first

For years, skills-based talent strategies were seen as an aspiration. Today, thanks to AI and data-driven insights, they are a business imperative.

We believe organisations that embrace this shift will not only outmaneuver the competition but also future-proof their workforce in an era of rapid transformation.

As the relationship between AI and human talent deepens, the skills movement will only accelerate, creating a smarter, more resilient and more inclusive world of work.

IT professionals suffering from burnout

Almost three quarters (73%) of European IT professionals have experienced work-related stress or burnout.

THE WELLBEING of European IT professionals is at risk, as almost three quarters (73%) have reported experiencing work-related stress or burnout. That's according to new research from ISACA, the leading global professional association helping individuals and organisations in their pursuit of digital trust.

This work-related stress is manifesting in different ways, with three in five (61%) citing a heavy workload as a contributor, as well as tight deadlines (44%) and lack of resources (43%). Nearly half (47%) found that difficult or unsupportive management were impacting workplace wellbeing.

Alongside these internal issues, external challenges including the wider skills gap in the sector mean that more work is being placed on the shoulders of existing staff.

Nearly half (45%) of European IT professionals decided to pursue a job in the sector because they enjoy the problem solving and creativity aspect, and 47% choose to remain in their current job because they find it to be interesting. Working in IT also offers good career development, with over two thirds (68%) of professionals surveyed having had a salary increase or promotion within the last two years. But for those looking to enter the sector, it can prove difficult - 30% of IT professionals said that specialised skills required for specific IT areas is the third highest challenge in Europe.

Chris Dimitriadis, Chief Global Strategy Officer at ISACA, said: "With skilled employees in such high demand, it is in companies' best interests and simply the right thing to do to make sure the tech workforce feels supported, motivated, and invested in. Younger IT professionals are switching jobs at a much higher rate, highlighting the



need for better retention strategies, including clear career growth pathways and a focus on work-life balance. At the same time, experienced professionals must be given the support they need to stay engaged and continue contributing their expertise. A balanced, well-supported workforce is key to sustaining the industry's growth and innovation."

Another frustration for a quarter of IT professionals (24%) is a lack of mentorship or guidance when entering the sector. Only 15% of European IT professionals have a mentor at all. This is despite over three quarters (76%) feeling that good mentors or role models are important to them.

That's not to say that progress hasn't been made in the sector more broadly. European IT professionals recognise the benefit of qualifications in furthering their development – 90% have participated in certifications to advance their career, and almost three quarters (74%) said that their employer provides or pays for certifications as part of their career development.

Although these are steps are in the right direction, for as long as the cyber skills gap continues to create wellbeing issues, hiring the right staff and providing mentorship and career development opportunities will be key to building a productive and satisfied workforce.

Sarah Orton, UK and Europe lead for ISACA's SheLeadsTech initiative, said: "It's clear that those working in the IT sector enjoy their roles but are being stretched to their limits by the persistent skills gap, underfunding, and a rapidly evolving and demanding sector.

"There are practical steps businesses can take - by creating mentorship programmes, investing in training and certifications, and establishing more accessible entry-level programmes, they will relieve common pain points and improve areas of employee fulfilment and satisfaction. With this kind of support, businesses can build a more motivated, productive, inclusive and equitable workforce – in turn building cyber resilience."

Companies that use IT cost optimisation to fuel innovation see improved return on investment

Businesses that create a cycle of savings and investment in innovation are 2x as likely to report improved ROI.

SOFTWAREONE HOLDING has released its new research “Driving Business Outcomes through Cost-Optimised Innovation”. There is a significant opportunity for companies of all sizes but in particular for those with revenue between \$500 million and \$5 billion, to optimise their IT costs and surge ahead in innovation.

The research shows that companies leading the way in IT cost optimisation and innovation are twice as likely as others to see an improved return on investment (50% vs 26%), report higher profitability (35% vs 23%), and faster time to market (43% vs 26%).

The new SoftwareOne study, conducted by an independent global research firm, investigates IT cost management and innovation best practices for mid-market companies.

The research surveyed organisations in 12 countries and across six industry sectors in North and Latin America, Europe and the Middle East, and the Asia-Pacific region. Survey respondents were classified into three categories — Optimised Innovators, Aspiring Innovators, and Initiating Innovators — based on their reported levels of progress in optimising IT costs and building a modern IT foundation.

While 48% of executives at mid-sized companies lack the budget or are unsure they have the budget to fund the next round of innovation, Optimised Innovators apply seven best practices to achieve results:

- Building a modern IT platform.** Optimised Innovators are well ahead of other companies in installing a modern IT foundation for driving ongoing cost optimisation and innovation.



- Investing in key digital initiatives.** Over the next two years, Optimised Innovators plan to significantly outspend other companies on critical technologies. The gaps were most evident for spending in network security, automation, and cloud and SaaS management.
- Prioritising data security and privacy.** Optimised Innovators use nearly every cybersecurity solution more often than others.
- Building a cloud-based infrastructure.** More than two-thirds have made significant progress in building a cloud-based infrastructure, and more than half have moved their apps to the cloud and migrated core processes. A similar percentage have established governance, compliance, and security policies. Over the next two years they plan to have 70% of their software applications and workloads in the cloud, as well as 56% of their custom applications.
- Closing the AI gap and moving ahead with adoption strategies to automate processes, improve decision-making, internal processes and customer engagement. 84% are at mid- or advanced levels of using AI for internal processes and 71% for customer engagement.
- Developing a GenAI first-mover advantage. Optimised Innovators

are nearly twice as likely as others to be at mid- or advanced implementation of GenAI for internal purposes and are considerably further ahead for customer engagement.

- Mastering the practice of IT cost management.** Optimised Innovators are ahead of their peers across nearly all areas of cost management, having made significant progress in monitoring and cutting operational, software licensing, and IT infrastructure costs.

Over the next two years, Optimised Innovators expect to make the most progress in sustainability, aligning FinOps with sustainability practices to optimise resource usage, reduce waste, and cut energy costs.

“Aligning the business benefits of innovation investments with opportunities to strategically optimise IT estates is critical to success.

Our study suggests that there is a clear opportunity for companies to optimise to innovate,” said Oliver Berchtold, President of Software and Cloud at SoftwareOne. “Having defined innovation priorities that drive business outcomes, companies can have a more informed understanding of their IT landscape with an end-goal in mind.

“This includes analysing software licenses, cloud environments and custom applications to identify areas for optimisation.

“This process will free up resources to invest where it matters most to the business, whether it be GenAI adoption, security solutions, or accelerated cloud transformation. Bringing these opportunities into reach serves as a catalyst for growth.”

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.managedservicessummit.com>



ITEUROPA





BPA or RPA? Maybe you need both

comparing BPA and RPA, when to use them, and when they work well together to bring about business change.

SATISH THIAGARAJAN, FOUNDER AND CEO OF UK CONSULTING FIRM BRYSA

PROCESS AUTOMATION might not be new. In fact, from the time of lean manufacturing, assembly-line production and more recently, the communications revolution, process automation has been in use. It has helped businesses improve efficiencies and reduce costs by leaps and bounds. Today, as businesses aspire to streamline workflows in their systems, Business Process Automation and Robotic Process Automation might just be the right tools. But what is the difference between them, and are they complementary?

Business Process Automation

Business process automation or simply BPA, is used to automate workflows that improve the efficiency of a process across an organisation, from end-to-end. Rather than focussing on a distinct individual task it encapsulates the whole process from end-to-end across the business and departments.

An example of this could be invoice processing. If a company implemented BPA, that process could capture a sent invoice, extract key data and then validate it against internal sales systems. If the invoice matches, it could be automatically sent for payment approval, and otherwise directed to a team for review.

Using BPA in this way can save hundreds of business hours a year, enable more rapid processing of invoices and better customer service experience for resolving invoices submitted with errors.

Robotic process automation

RPA, short for Robotic Process Automation, is another process automation technology that works via software (ro)bots. Unlike BPA which automates business processes, RPA imitates human tasks that would take place on a computer by following a set of predefined rules. For example, an RPA bot can:

- Log into systems
- Navigate online pages or documents
- Input and extract data
- Mimic any other interactions humans have with computer systems.

One example of RPA, could programming a bot to assist with onboarding new hires. When a candidate accepts an offer, the bot would automatically trigger a series of actions. It first creates a new employee record in the HRMS (Human Resource Management System), then sends a welcome email with links to complete forms. The same RPA would update IT with a request to set up email accounts and hardware access, before logging the progress of the onboarding process in a tracking spreadsheet used by HR staff.

Choosing between BPA and RPA

The choice between BPA and RPA is not really a complicated one. All you need to do is consider a few factors, like the scale of automation required, costs, and the complexity of the processes involved. For example, BPA is ideal for organisations looking to optimise their entire workflows across multiple

departments. It involves integrating disconnected systems like CRM, ERP, and HRMS to eliminate inefficiencies. Common use cases of BPA include:

- Optimising order management
- Setting up multi-level approval workflows
- Streamlining regulatory compliance processes

On the other hand, RPA is best for automating specific, repetitive tasks. It's especially useful for short-term automation needs or working with legacy systems that lack integration capabilities. It works within existing systems without requiring significant redesign. So, it is a good choice if you are looking for a quick and cost-effective solution. Common use cases of RPA include:

- Extracting data from invoices
- Automating email notifications
- Automated report generation

Benefits of Combining BPA and RPA

Both BPA and RPA can complement each other. RPA can streamline individual tasks within a BPA-driven framework. This ensures immediate and long-term process efficiency. RPA handles repetitive, rule-based tasks, such as data extraction or email notifications, while BPA focuses on end-to-end workflow optimisation.

Together, they enable you to streamline processes at both micro and macro levels. For instance, RPA bots can efficiently collect and input data, which BPA systems then use to trigger complex workflows across departments. This integration minimises human intervention, reduces errors, and accelerates overall process execution.

The combination also ensures flexibility and scalability for your business. RPA can quickly address specific pain points and deliver immediate productivity boosts. BPA provides the foundation needed for long-term process improvements.

Leveraging BPA and RPA

To effectively leverage BPA and RPA, you need to choose a toolset that can seamlessly integrate with a wide range of systems through adapters, APIs or other standards. Many tools come pre-configured for a range of the most popular business apps. Just think about the number of applications used by staff in different departments and roles in your business and you'll quickly be in double figures.

Adaptability is also key. There will be cases where you want to move quickly up implement or update BPA and RPA rules. The best tools do this through the use of visual tools that help you quickly design end-to-end workflows as a logical sequence of events.

Finally, scalability matters too. How many users or transactions will your tool need to process? What

happens when a new branch is opened, or a rule change needs to be rolled out globally? Any tool chosen needs not only to be able to cope with a workload, but possess the management tools that allow you to test, roll out and roll back RPAs and BPAs across your estate, however large or distributed.

Legacy applications

Whilst a business may use a number of enterprise apps, many still those one or two apps that they do not dare get rid of. It might be an application that runs as part of a piece of old (but essential) production line equipment, or even a mainframe, but BPA and RPA can still be used here.

Rich RPA and BPA platforms such as Salesforce work with legacy systems to streamline processes like data entry and data extraction by mimicking human actions to interact with applications, documents, and databases. Some platforms are very rich and even allow Optical Character Recognition (OCR), web and image search, and use APIs to automate data retrieval and processing from various sources, including spreadsheets, emails and web pages.

It's doesn't need to be binary choice

At a time when everyone is obsessing over AI, which can seem like a hammer to crack a walnut, BPA and RPA still have a role to play. If you have repetitive activities or whole business processes in your organisation that have become an unnecessary 'time suck' then BPA, RPA, or a combination of the two can quickly save huge amounts of time, improve the experience for your customers and suppliers, and allow staff to spend their time on higher value tasks. One can argue that this is even a prerequisite for successful AI implementation, since good AI Agents and systems can only be implemented on good data and processes.





Keep on security running - why compliance has to be continuous



The cost for security breaches continues to rise. According to IBM's Cost of a Data Breach Report for 2024, the average cost for a breach was \$4.88 million, a rise of 10 percent year on year. With so much

at stake, it should not be a surprise that governments are closely scrutinising their regulations around security. The European Union has introduced the NIS2 Directive to update guidelines for all organisations deemed to provide critical infrastructure across 18 sectors, from the usual suspects like banks, retailers, healthcare and utilities through to IT and cloud services providers that underpin digital business processes.

BY NATHAN COLLINS, REGIONAL VICE PRESIDENT EMEA, NETALLY

THE UPDATED NIS2 Directive supports organisations to enhance their cybersecurity capabilities, develop their risk management approach and have reliable reporting in place around those risks. At the same time, it sets rules for better cooperation and information sharing between organisations. The overall goal is to raise the quality of security and risk management across the board.

What makes compliance difficult

Meeting the needs of regulation like NIS2 should be high on the priority list for companies. However, the amount of work needed to get compliant should not be underestimated. When security is so hard to achieve in the first place, let alone to keep in place, how can teams improve their performance? We need to look at the obstacles we face and evaluate whether our current approaches are the right ones.

First of all, it is important to recognise how tough it can be to know with confidence what assets or endpoints you have across your environment. The exponential growth of edge-connected devices (headless Internet of Things, operational technology, industrial controls, and other unmanaged assets)

has added to the burden that exists for IT security and operations teams.

All those devices must be connected to the corporate network to work effectively. Without the proper security processes in place, those environments can have unsecured connections in place, which can pose risks. The ubiquitous nature of that connectivity can also be a challenge, as attackers can use unsecured assets to reach locations on the network that would otherwise be secure.

Alongside this, the network architecture is becoming increasingly complex to manage over time. Any device on the network - and the network itself - can have misconfigurations due to human error that can lead to gaps in security. To stay resilient and comply with NIS2, you must find those oversights and ensure you stay ahead of any problems.

Where does your data come from?

You must identify what is currently installed to address these challenges and maintain network security. After this, you have to keep that inventory up to date over time. The challenge is that all the tools typically used to piece together this inventory can miss out on discovery of all endpoints.

Traditionally, security teams rely on vulnerability management (VM) tools to understand what assets they have installed and - most importantly - what issues need to be addressed.

However, while VM tools can theoretically provide this insight, the discovery process can easily break down. The further away that assets are from the central starting point for VM discovery, the more likely they are to be missed, resulting in individual assets or even entire network segments being overlooked.

This can be due to the network architecture itself - networking techniques such as asymmetric routing, Network Address Translation (NAT) set-ups configurations or hub-and-spoke design topologies can lead to missed assets, as can firewall settings. Similarly, network media converters can cause un-discovered paths. Common misconfiguration examples include putting switches in the wrong VLAN so they don't have an IP address in the VLAN segment under test. This leads to a VLAN mismatch going out so those assets on that segment will not respond to a broadcast.

Alongside VM tools, network management products can provide insight into all the infrastructure in place across the network, from switches, routers and firewalls through to Wi-Fi Access Points.

Typically, these products work by periodically collecting data from all the devices on the network using SNMP, packet sniffing, flow data, syslog, APIs, or agents. These network management tools

Alongside VM tools, network management products can provide insight into all the infrastructure in place across the network, from switches, routers and firewalls through to Wi-Fi Access Points. Typically, these products work by periodically collecting data from all the devices on the network using SNMP, packet sniffing, flow data, syslog, APIs, or agents. These network management tools can also be configured to alert on configuration changes, so that any significant change is flagged automatically

can also be configured to alert on configuration changes, so that any significant change is flagged automatically.

While network management tools can communicate with network infrastructure elements, they frequently cannot discover all the endpoint devices that are on the network. In addition, they can be difficult to set up and configure, requiring specialized knowledge and training to use effectively, and frequently generate false alarms. This makes compliance harder over time.

Alongside VM and network management products, security teams frequently rely on their endpoint management tools to provide that level of visibility. Typical products used include network access control (NAC) tools, managed detection and response (MDR) solutions and endpoint profiling



tools. These tools vary - some deploy agents out to the endpoints to provide information back, while others use network traffic analysis to passively view endpoint traffic or flow.

Looking at endpoint management alone can be a challenge, especially when it comes to defining what an endpoint actually is. Common devices like PCs, tablets and servers can have agents installed on them, but how about other devices that would be installed in edge environments?

Operational technology systems like industrial control systems and headless IoT devices can't support agents, and other items like IP cameras, building control systems and sensors can also exist at the edge. Those systems should be tracked and kept secure just like a traditional endpoint asset. Any device without that agent can create a blind spot that malicious actors could exploit.

There can also be a cost and complexity element to this side. For instance, endpoint management tools can be a lot more expensive to procure and cumbersome to implement due to the requirement to span or tap ports in order to work.

Additionally, the amount of data generated by these solutions must be saved, stored, and analysed over time, which adds another layer of overhead.

How to plan ahead

If you can't get a full picture of what you have, you can't ensure it is secure and resilient. To build an effective approach to security and compliance, you have to start with a complete asset inventory. Using a combination of tools, you can get that accurate inventory in place that will be the basis for your long-term planning.

One consideration is that, while a centralised inventory can be carried out successfully, there is no substitute for getting out to the edge and carrying out testing within each location. Local network testing can corroborate your approach, but also find additional networks or connected devices that have to be brought into scope.

This local testing should be a regular part of your strategy so that you can keep your security and compliance models up to date with your real-world environment.

Compliance frameworks like NIS2 provide effective guides for security and resilience. At the same time, they generate additional work for security and networking teams to manage. By understanding the gaps that can exist in asset programmes, you can reduce the potential for gaps in your planning and prevent issues before they arise. More importantly, you can make the compliance process easier and prove that you are following those best practices.



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.



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.managedservicesummit.com>

Angel
BUSINESS COMMUNICATIONS

ITEUROPA

ANGEL
EVENTS



What does risk mean to you?

However mature you are as an organisation around security, there are always improvements that can be made. Focusing on risk - what issues exist and what they may cost the business if something goes wrong - makes it easier to work across teams to make those improvements.

BY MATT MIDDLETON-LEAL, MANAGING DIRECTOR NORTHERN EUROPE, QUALYS

THERE'S a famous quote attributed to George Bernard Shaw: Britain and America Are Two Nations Divided by a Common Language. In the UK, chips are french fries, while US potato chips are crisps. While they are all potato products, they are very different and you don't want to be disappointed! Without that understanding, it's easy to miss some of the meaning.

The concept of risk is the same. Say "risk" to a Chief Information Security Officer, a Chief Finance Officer and a Compliance leader, and they will have very different ideas in mind of what you mean. The challenge around risk is that it affects the whole business, so silos or misunderstandings can have a material impact.

So how can we overcome this problem, and get more understanding across security, finance and compliance? How can the CISO, CFO and Compliance function leaders understand each other better?



Centralise your risk operations

The hurdle to get over is how data is siloed across the organisation. Enterprise IT teams support multiple different digital platforms that are in place from legacy client-server deployments all the way through to modern cloud applications and software containers. Each and every application will

have huge numbers of components that all have to be tracked. Any potential outage or software vulnerability will have an impact on the business, so standardising on how much that will cost is an essential move to get everyone to the same point of understanding.

Putting a cost on a failure - whether that is a full scale data breach due to a software vulnerability, through to downtime needed to prevent an attack - is a critical step to make this successful across the business. This exercise is called cyber risk quantification - for many CISOs, this is something that they will need to carry out rather than delegate to their security analysts in future, as it ensures that they can have full and frank conversations with the rest of the business around risk. It also helps the CFO and the Compliance team speak around security risks in a common language that they and their peers can understand, rather than going into their own jargon. Linking it to money makes it easier to explain risk to the rest of the business as well.

Centralising this data and creating a risk operations centre (ROC) to manage this process enables you to get everyone together. While each team might need a different view on the data itself, having one central point to manage and control operations makes responding easier to coordinate and prioritise. Similar to a security operations centre, or SOC, the

ROC approach involves having the right people able to make decisions based on the right context.

Improving results around risk

The goal for a ROC deployment is to improve how risk is handled, processed and ultimately reduced across the organisation. For the CISO, risk reduction comes from better understanding of how much risk the business faces at any given point due to software vulnerabilities or particular threats, and how that level of risk changes over time. By integrating the ROC as a place where decisions on priorities get made with the SOC to take care of security and remediation programs, the CISO can direct resources to the issues that need to be addressed urgently. This also makes it easier to collaborate across software development, IT operations or other teams that are responsible for carrying out mitigations or updating assets, because they will have the context for those decisions as well.

For the CFO, getting more insight into risk across the business provides them with a better understanding of the financial impact that potential events can have. Rather than looking at data that makes sense to IT teams, the CFO can draw a direct line between risks and mitigations. While this can support decisions around IT and security budgets, it can also be used to plan around other mitigation strategies, like choosing the right cyber insurance approach and buying the right levels of coverage

rather than policies that sound right, but would not pay out adequately in the event of a data breach or other event.

For Compliance teams, working with the rest of the business on risk helps them to plan ahead around current and future regulation. Companies involved in critical national infrastructure in the EU and beyond have to implement resilience policies to meet NIS2, while those in finance and banking have to comply with DORA from January 2025. Both of these regulations stipulate specific requirements around security and resilience planning. From a risk perspective, any failure can lead to significant fines. Further regulation around product safety and AI may also affect businesses too. Understanding that potential impact and where gaps exist is harder when you are working in a silo, so having real world financial impact data to use will support any future planning and investment.

However mature you are as an organisation around security, there are always improvements that can be made. Focusing on risk - what issues exist and what they may cost the business if something goes wrong - makes it easier to work across teams to make those improvements. By speaking a common language around risk that is directly linked to financial impact will ensure everyone can focus on how to make those improvements, and ensure they stick over time. With a ROC, everyone can speak the same language about reducing risk.



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

**ANGEL
EVENTS**



AI, data and software: a new era of automotive safety

Imagine a world where the fear of road accidents is a distant memory. A world where cars intricately understand their surroundings, can see far into the distance even in complete darkness, and sense danger before it happens. Cars that can predict future events in a fraction of a second, seamlessly communicating with other vehicles, infrastructure and humans.

BY ALWIN BAKKENES, HEAD OF GLOBAL SOFTWARE ENGINEERING, VOLVO CARS

HERE AT Volvo Cars, we've been envisioning a safer future on the roads for nearly 100 years. Because if we can't imagine the future, we can't build it.

I'm excited to see new technological advancements making roads and cars safer than ever before. These innovations are ushering in a new era of safety. Let me explain.

The history of automotive safety

Back in the 1950s, automotive safety innovations were passive by design – they protected passengers when an accident happened. Safety belts, airbags and strengthened safety cages are all great examples of proactive safety innovations that have saved lives around the globe.

In the 1970s, active safety features began to be adopted in cars. These features were developed to help prevent accidents in dangerous situations by assisting drivers in detecting and avoiding crashes. Innovations such as Blind Spot Information System

(BLIS), adaptive cruise control and anti-lock brakes emerged during this era, significantly improving car safety.

Data makes a big difference

It's no secret that data has long held the answer on how to improve automotive safety. It has driven numerous safety innovations over the years, not just for Volvo Cars but across the entire industry. The Whiplash Injury Protection System (WHIPS) and Side Impact Protection System (SIPS) are good examples of our safety innovations inspired by data collected from crash sites since the 1970s.

But in the past, collecting the necessary data hasn't always been easy. Manual data collection is labour-intensive, and it can be time intensive to contextualise and turn into insight, even with the most fine-tuned, consistent processes in place. Fortunately, new technological advancements have helped to address these issues.

Core compute has changed the game

New cars today are more like super computers on wheels. They have highly sophisticated computing architectures connected to advanced sensors that help understand what is happening in and around the car better and faster than ever before. For context, [according to industry analysis](#), a typical new car today has more than 150 million lines of code and processes 25GB of data per hour. That's 1,000 times more lines of code than Apollo 11, which landed on the moon.

For car manufacturers that have begun their software-defined journey, the data collected by core compute architectures is invaluable. It allows us to contextualise this data, unlock new learnings, train future safety models and roll them out globally. For Volvo Cars, this is the real value of the software-defined car.

The transition to the software-defined car running on a core compute system is like adding a superpower of real-world, real-time insight and the ability to write new instructions back to the product to respond even better the next time around. It creates a future where cars can start to learn together as one, growing smarter from each other's individual experiences.



Becoming software defined

The transformation I've described above is perhaps one of the most challenging that any car manufacturer will ever undertake. It represents an even greater milestone than the transition to electrification.

In addition to the innovations mentioned, it requires a completely new organisational infrastructure. This includes creating a software layer that can run across all cars and connect seamlessly with all partner and smart city ecosystems. It requires the most advanced connectivity to enable car communication, cybersecurity protocols to ensure safety, edge computing to reduce latency and a data warehouse to power machine learning.

It requires a complete change in mindset and culture, thinking software-first. It requires the bravery to journey into the unknown and the ability to convince leaders that this is the correct path to take. Success is about continuous innovation,



hard work and collaboration, empowering software engineers to make meaningful change in the world by combining energy, matter and code in new ways.

And finally, it requires vision and purpose, just like the one I began this piece with. Success in the modern world isn't about using technology as a status symbol. Nor is it about embracing innovations that always accelerate the pace of life into a blur or contribute towards an unsustainable way of living (for the planet or for our drivers). When used to its full potential, technology has a much more important purpose – it can save lives and elevate the quality of life.

Technology with purpose

At Volvo Cars, we have the vision, purpose, technology, heritage and roadmap. Our human-centric approach to technology means we use it to make meaningful change in the world – improving safety and elevating the quality of life for our drivers. We've been relentlessly using data to improve safety while embracing new technologies that will allow us to raise the bar further.

Thanks to our recent technological transformation, we can harness the power of AI, data and software to build safer cars more efficiently than ever before, bringing us closer to our ambition of a zero-collision future.



Assessing cloud security strategies: reactive, proactive, or responsive?

Cloud security market growth shows no signs of slowing down. According to Fortune Business Insights, it is projected to reach \$43.74 billion by the end of this year and surpass \$63 billion by 2028. As the cloud security market grows, so do the opportunities and attackers' tactics and techniques, which are becoming increasingly sophisticated, relentless, and fast.

BY CRYSTAL MORIN, CYBERSECURITY STRATEGIST AT SYSDIG

MANY ORGANIZATIONS now ask themselves the same question: Are we prepared to meet these security challenges head-on, or are we merely reacting to incidents as they arise? Let's explore the distinctions and determine how to best position your organization for future security success.

There are a plethora of different cloud security solutions all vying for attention. Adding to the chaos, many of them have different acronyms and solve all or part of the cloud security problem. From specific solutions like cloud workload protection platforms (CWPPs), cloud security posture management (CSPM), and cloud infrastructure entitlement management (CIEM) through to all-encompassing cloud-native application protection platforms (CNAPPs) — are you confused yet?

In a dynamic market for a dynamic environment, organizations must continuously assess and adapt their cloud security strategies to ensure they're using the right tools and making the right calls. Looking at your existing strategies and processes can simplify those decisions. There are

three main elements to consider: reactive security, proactive security, and responsive security.

Reactive security

For some security teams, security strategy is simple: when they find problems in their tech stack, they fix them as fast as possible. This approach involves building and managing effective processes for new issues or vulnerabilities as they are discovered, whether in application components, software container images, or the cloud infrastructure used to host them. This approach is effective at dealing with these problems as they come up, but it presents a potentially stressful environment for their security team.

Relying solely on a reactive security strategy is risky because if your reactions aren't fast enough — and they're likely not given that cloud attacks unfold in 10 minutes or less — your organization is dealing with the fallout of a breach. To improve your reactive security processes, you need to use real-time threat detection, implement measures that streamline





incident response, and further reduce the time between finding and fixing problems in your tech stack.

To refine these processes, consider using automated tools, fostering strong communication with developers, and conducting regular readiness drills. Even with only a reactive security strategy these enhancements can more effectively mitigate the risks of a dynamic cloud environment.

Proactive security

For security teams that opt to be proactive and solve potential problems in advance, integrating security into the software development process is essential. By embedding security through security-as-code (SaC) and policy-as-code (PaC) rule sets, teams can ensure security is built into the source code from the outset. This enables the security team to implement and maintain a proactive security posture, and it also provides developers with the tools and guidelines needed to create secure-by-design applications and infrastructure.

The goal of a proactive security strategy is to avoid an excessive amount of stress on the security team and — perhaps more importantly — breaches.

Another means of enhancing a proactive security posture is monitoring continuous integration and continuous deployment (CI/CD) pipelines and the images used in these systems. You can often spot potential issues within those environments and remediate them before they go into production.

While a proactive security strategy offers many benefits, relying solely on it can also be risky. Even the most thorough proactive measures can miss unexpected threats or overlooked vulnerabilities as the dynamic cloud and threat landscape change,

and 10% of malicious images are missed with pre-production scanning alone.

Responsive security

When looking at reactive and proactive security strategies, it should be clear that both are necessary to properly secure cloud environments and prevent attacks. While you might want to prioritize being proactive, the truth is that new threats and risks will always arise that require a reactive strategy. And though you might have an all-star incident response team, you can always find ways to more effectively use your resources by proactively detecting and suggesting fixes for software vulnerabilities.

What you need is the right mix: reacting as needed and planning ahead wherever possible. Using the 80/20 rule, you might find that you can cover the majority of concerns by being proactive and leaving your teams more time to concentrate on those reactive events that represent the most risk to your organisation in the shortest amount of time.

Start with full visibility of the IT assets running in your cloud environment, including the initial container builds in your repositories or libraries and the production workloads and cloud workloads in your infrastructure. However, even though that level of visibility into your stored images will tell you a great deal, it still won't tell you exactly what is running in your environment at any given point in time. For a cloud environment, the ideal starting point for a responsive security strategy is runtime security.

Runtime security

Cloud environments are dynamic — developers are constantly making changes to applications and containers in dynamic cloud environments. Containers may drift from their initial, secure builds

to versions that contain vulnerabilities. Running software may also call additional resources not captured in the software bill of materials (SBOM), leading to untracked dependencies. Cloud applications consist of various components and services for which security monitoring data must be gathered and is not inherently available.

Runtime security provides crucial insights into what is actively running within your environment, allowing the security team to properly prioritize their proactive security strategy. Our previous research found that 87% of container images have high or critical vulnerabilities, but only 15% of these are tied to loaded packages at runtime.

This allows teams to enforce policies on which processes are permitted to run and which accounts are allowed to run certain tasks. Through the use of proactive elements such as continuous real-time monitoring and machine learning, runtime security can anticipate potential threats by identifying anomalies and deviations from baseline behaviors, preempting attacks and strengthening an organization's proactive security posture.

Our Threat Research Team (TRT) found that, on average, attackers can exploit a cloud environment within ten minutes of gaining initial access.

This rapid exploitation underscores the necessity for a reactive security strategy in conjunction with your comprehensive proactive security strategy.

Getting ahead of that timeframe is key, and by correlating threat intelligence with runtime vulnerabilities, policy violations, and other information, security teams can quickly detect and respond to threats before they become full-blown incidents.

Getting the right mix

Reactive and proactive security strategies are essential for improving security posture, but they can quickly lead to information silos, inefficiencies, and missed opportunities to be more effective.

Incorporating runtime insights into a responsive security strategy bridges the gap between reactive strategies, like incident response, and proactive strategies, like vulnerability management and threat anticipation.

Ultimately, whether you opt for a reactive, proactive, or responsive security strategy, the key is to ensure that it aligns with your organization's goals, resource limitations, and threat landscape. It's up to you to position your organization for security success in the dynamic environment of the cloud.



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

**ANGEL
EVENTS**

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>



ITEUROPA





How the Vulnerability Operations Centre serves as an essential mission control for vulnerabilities

The vulnerability management 'to do' list can feel like a perpetual loop. No sooner have the latest batch of security updates been handled than it's time to start over again.

BY PIERRE SAMSON, CRO AT HACKUITY

INDEED, security teams weighed down with manual processes and siloed structures are likely to find they can't even complete one set of vulnerability management tasks without others needing urgent attention. In the absence of a coordinated strategy, critical risks mount up and begin to slip through the cracks, increasing exposure to attacks. It's time for a shift. Security teams must transition from ad-hoc urgency to a mission control mindset powered by adopting a Vulnerability Operations Centre (VOC) approach. The next evolution of the SOC, the VOC enables teams to centralise, streamline, and strengthen vulnerability management.



Why traditional vulnerability management is falling behind

The number of Common Vulnerabilities and Exposures (CVEs) has been increasing steadily over the last few years, but the growth is reaching exponential rates. More than 40,000 new CVEs

were recorded in 2024 alone, averaging at around 108 new threats every day of the year.

Any vulnerability management setup still relying on manual processes to track and fix vulnerabilities has an impossible task ahead of them. Teams that must crawl through spreadsheets to work out their next priority will never get close to getting through their backlog, let alone working out a proper set of priorities.

Many vulnerability management strategies are also over-reliant on single sources of truth for discovering new vulnerabilities and prioritising their activity. The National Vulnerability Database (NVD) has often served as the go-to source of information but last year suffered a major slowdown due to a lack of resources and funding, causing a large backlog of unprocessed vulnerabilities. Organisations without the ability to proactively identify and prioritise vulnerabilities found themselves without a clear

direction. As highlighted by CISA's Vulnerability Response Section Chief earlier this year, security teams need clarity, context and actionable insights to make vulnerability management workable.

These issues are compounded by siloes in both tools and processes. Teams must often move between multiple sets of overlapping but disconnected tools, wasting time and leading to gaps and duplicated effort. Different teams such as security, IT and DevOps may also be working in isolation, leading to more redundancy and misaligned priorities.

Taken together, this results in a highly reactive, fragmented approach that leaves organisations at risk of missing high-priority vulnerabilities which are being actively exploited by threat actors. Organisations still struggling to get to grips with vulnerability management urgently need a more organised and efficient approach. This is where the VOC comes in.

Introducing the VOC as mission control

As the name might suggest, the Vulnerability Operations Centre takes its cues from the Security Operations Centre (SOC). Just as SOCs establish a single point of visibility and control for identifying and responding to security risks, the VOC creates a consolidated, holistic approach exclusively to vulnerability management.

The strategy has gained significant traction over the last couple of years, and more CISOs are now on the path to implementing a centralised hub for vulnerability management. The goal is to achieve real-time and contextualised visibility into all vulnerabilities, assets, and risk levels across the entire business.

It also bridges SOCs and vulnerability management programmes, unifying stakeholders across security, IT, and DevOps teams.

The key to achieving all this is the implementation of a highly automated approach to vulnerability management. Data from multiple sources, such as external threat intel feeds or databases like the NVD, and internal scanning tools and asset inventories, is aggregated together and de-duplicated into a single pool.

Vulnerabilities are then prioritised based on several factors, including severity, exploitability, and asset context. Crucially, this should be a highly bespoke process customised to the organisation's specific risk tolerance, rather than a one-size-fits-all approach. Priorities need to match the reality of business operations closely.

Key advantages of a VOC for modern security teams
A fully operational VOC can immediately start delivering tangible business benefits. Crucially,

teams will be able to pinpoint the vulnerabilities that really matter and tackle them quickly. Not all CVEs are created equal, and context is critical for proper prioritisation. For example, a mid-severity vulnerability on an exposed system may be riskier than a critical flaw with no exploit available on an isolated server.

With accurate and reliable data to guide them, the team will always be addressing those exploits with the greatest risk factor based on asset exposure, exploit availability, and business impact to focus efforts where they're needed most.

The VOC also enables a highly automated and efficient operation. Vulnerability triage, risk analysis, and alert prioritisation are all prime areas for automation, freeing security teams to focus on strategic decisions.

This not only enables the team to cut through the noise to identify and respond to the most critical issues, but also helps avoid alert fatigue, keeping personnel from feeling burnt out by an endless list of manual tasks.

These tactical benefits add up to the strategic result of greater security and resilience for the business. The enterprise has a reduced chance of suffering a breach and all the operational, financial and legal issues that come with it. This proactive stance helps reframe vulnerability management from a necessary evil to a business enabler that helps the company operate with more freedom.

From firefighting to foresight

By establishing a centralised hub to act as mission control for all things vulnerability management, VOCs give security teams the tools to anticipate and prevent attacks, not just respond to them.

While CVE volumes are only likely to keep increasing year over year, those armed with VOC's real-time intelligence and automated workflows can safely ignore the vast majority and confidently focus on the handful that pose a real risk to their business.



How can businesses avoid cybersecurity blind spots in 2025?

Cybersecurity incidents in 2024 reinforced a hard truth: most breaches stem from preventable security failures rather than sophisticated attacks. Once again, last year, attackers relied on well-known tactics like phishing and credential theft, often using generative AI to launch these attacks quickly and at scale.

BY DR YVONNE BERNARD, CTO AT HORNETSECURITY



A 2024 Hornetsecurity ransomware attack survey revealed that over two-thirds (66.9%) of respondents said the emergence of generative AI increased concerns that their organisations would become ransomware targets, with small businesses (55.3%) becoming the prime target of these types of attacks in Q3 alone.

With limited cybersecurity expertise and resources, small businesses often struggle to defend themselves against evolving threats. But for any organisation, understanding the most common security gaps is critical to strengthening resilience and preventing future breaches.

The key question now is: what security gaps should businesses prioritise to ensure they don't fall foul of future cybersecurity attacks?

Phishing and credential theft

A UK government survey from April 2024 revealed that 50% of all businesses and 84% of large enterprises experienced a cybersecurity breach or attack in the past 12 months. Of these, phishing was by far the most common attack vector, affecting 84% of businesses and 83% of charities.

Many phishing attacks rely on reverse proxy-style credential theft, whereby social engineering and malicious links are used to bypass authentication controls and compromise accounts. Yet, despite phishing's year-on-year dominance and the simplicity of their attacks, many organisations remain unprepared due to a lack of security awareness training.

While it is a must to have robust, next-gen cybersecurity solutions in place, all the latest firewalls, complex passwords, and best anti-malware solutions in the world won't be enough if the human defences are weak. Cybersecurity awareness training, which should cover different

types of phishing and credential theft attacks, is extremely important to ensure the 'human firewall' of a company is fortified.

Inadequate protection against chat-based attacks
Another security gap that businesses may not be aware of is threat actors' emerging use of real-time communication tools like Microsoft Teams to launch cyberattacks. These platforms have become new targets for phishing-style attacks, where attackers impersonate trusted contacts to distribute malware or steal credentials.

These chat-based threats bypass traditional email security measures and exploit the implicit trust employees place in internal communications. Most employees aren't trained to spot cybersecurity threats in these spaces, which means businesses are leaving blind spots that attackers are exploiting.

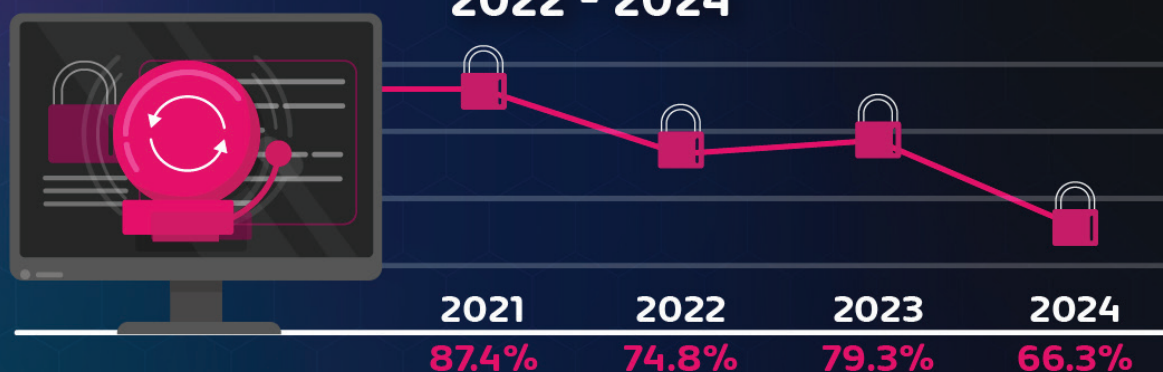
Compromised backups - when safety nets disappear
Another security gap businesses should prioritise is properly secured backups. These are critical safeguards against data loss and ransomware, but many organisations failed to secure them properly last year. In 2024, 16.3% of ransomware victims reported a ransomware payout to recover their data – a sharp year-on-year increase from just below 10%.

This increase highlighted an unpreparedness among organisations when it came to securing their critical data, particularly as ransomware attacks grew more sophisticated. Increasingly, attackers not only encrypted primary systems but also backup systems, which traditionally served as a company's final safety net, rendering these inaccessible.

To outpace modern threats, businesses need immutable backups that are stored in a way ransomware cannot alter or delete. If recovery plans do not account for ransomware targeting backups, then it no longer becomes a plan but a gamble, and

VICTIMS THAT RECOVERED THEIR DATA THROUGH BACKUPS

2022 - 2024



 HORNETSECURITY

© HORNETSECURITY 2024

in 2025, businesses cannot afford to roll the dice. The security gaps covered so far highlight the importance of a proactive strategy, whether that's security awareness training or ensuring backup systems are resilient. But what's the core principle or strategy that unifies these seamlessly?

'Zero trust' environment

Zero trust is a practical security approach that minimises risk and limits the impact of breaches. Instead of assuming certain users or devices are 'safe,' zero trust requires continuous verification and strict access control to prevent unauthorised access, whether from external threats or insider risks. There are three main components of zero trust, which should cover the security gaps that businesses often neglect or miss.

The three core pillars of zero trust call for:
Verify explicitly: authenticate and authorise every connection (even if it's coming from an internal network).

Assume breach: segment networks so that when a breach occurs, it doesn't automatically mean an organisation's entire network is compromised.
Adopt least-privilege access: ensure users only have the necessary permissions for their tasks.

However, there's a key problem with implementing zero trust. Granting access is easy, but continuously

reviewing and removing unused permissions is difficult. Employees and external parties often retain access long after it's needed, and the shift to cloud-based environments and remote collaboration has further complicated access management. It leaves the door open for potential breaches at any point.

This is where permission managers play a critical role. By automating access reviews, enforcing least-privilege policies, and preventing overdue permissions, businesses can continuously enforce 'zero trust' principles without overwhelming IT teams. That said, technology alone cannot replace the strength of a 'human firewall', a defence that is strengthened when the leaders in an organisation set the example.

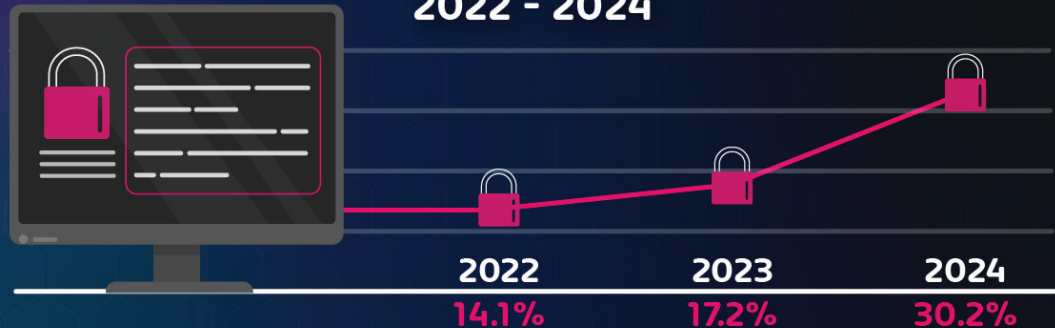
Why leadership buy-in is key to cyber resilience
Having a strong 'employee firewall' is crucial, and leading by example strengthens this. Leaders must recognise that cybersecurity is a business-wide priority, not just an IT issue. It demands clear accountability across departments.

Many organisations leave security concerns 100% in the hands of IT and/or their CISO(Chief Information Security Officer). A CISO's job is more than just 'secure everything' and take the blame for breaches. There is a very important human and business process component involved as well that requires input from company stakeholders. Instead

Another security gap that businesses may not be aware of is threat actors' emerging use of real-time communication tools like Microsoft Teams to launch cyberattacks. These platforms have become new targets for phishing-style attacks, where attackers impersonate trusted contacts to distribute malware or steal credentials

VICTIMS OF RANSOM ATTACKS THAT SUFFERED DATA LOSS

2022 - 2024



 **HORNETSECURITY**
© HORNETSECURITY 2024

of assuming security is solely a CISO responsibility, every business unit must take ownership of the security risks tied to the tools, applications, and data they manage. The finance department, for example, must assess the risks of the SaaS solutions they chose hand-in-hand with the IT department. HR must be accountable for the personally identifiable information (PII) they process. To build a genuinely cyber-resilient business, everyone must be involved. There's no point in the security team taking the blame and responsibility for mistakes that other departments might make.

Blaming security teams for breaches caused by poor security practices elsewhere is counterproductive. Cyber resilience is only possible when security is integrated into the company's broader risk management framework and when leaders set the standard.

Back to basics

In 2025, cybersecurity is about more than just technology or reacting to the latest AI-driven deepfake or phishing scam. It's about mastering the basics: vigilance, accountability, and a proactive mindset.

The most devastating breaches often stem from overlooked vulnerabilities, cutting corners, and preventable mistakes.

Businesses that prioritise security awareness, strict access control, and leadership-driven accountability will be the ones that remain resilient. In a world where breaches are inevitable, preparedness and awareness are the only true defence. The organisations that embed security into their core business strategy will be the ones that withstand future threats and thrive.

BARRIERS REGARDING RANSOMWARE TRAINING



17.8%
Too Time
Consuming
For End Users



14.4%
"Untrainable"
Users



12.3%
Too
Costly



10.6%
Too Time
Consuming
For I.T. Staff



7.6%
Training
Feels
Outdated

 **HORNETSECURITY**
© HORNETSECURITY 2024



Hybrid Multicloud as an operating model: streamlining enterprise IT

Whether scaling to meet demand, controlling costs, or boosting operational resilience, hybrid multicloud can provide the agility and control modern enterprises require.

BY SAMMY ZOGLAMI, SVP EMEA AT NUTANIX

ENTERPRISE IT environments are often a tangled web of data centre infrastructure, private and public cloud deployments, and, increasingly, edge locations. This variety offers organisations flexibility but introduces a new level of complexity that can drive up costs, limit scalability, and demand extensive management. Add to the “challenge mix” that data volumes are surging, new applications are constantly emerging, and digital transformation efforts are pushing both budgetary and operational demands into never-seen-before territory.

Where we find ourselves is in a world where customers are grappling with infrastructure that is increasingly complex, inefficient, and costly to maintain. To overcome these challenges, forward-thinking organisations are embracing a hybrid multicloud strategy as a unified operating model. With hybrid multicloud, companies gain a structured way to manage multiple environments as a single, adaptable ecosystem—one that maximises flexibility without sacrificing control or security.

It's an operating model that, when done right, extends beyond just an infrastructure shift; it ensures better data governance, helps optimise skills, and gives a business the agility needed to

adapt and change workload placement as and when the business demands it.

Implementing hybrid multicloud as the modern operating model

At its core, hybrid multicloud as an operating model integrates on-premises, private cloud, and multiple public cloud platforms into a single unified system. This unified model allows enterprises to adapt to changing workloads, optimise resource allocation, and maintain data governance across their environments. Workloads can be dynamically shifted based on cost, performance, or regulatory requirements, maximising operational efficiency.

Consider a retailer that needs rapid scalability during peak seasons like Black Friday or the last-minute holiday rush. Hybrid multicloud allows them to handle this surge by moving high-demand workloads to the cloud, then scaling back once demand normalises. This operational flexibility isn't just convenient; it's a competitive advantage.

The growing appeal of hybrid multicloud

The popularity of hybrid multicloud is evident: enterprises are increasingly adopting this model for



its ability to reduce IT complexity while maintaining a flexible approach to workload management. Industry studies indicate that most enterprises already deploy multiple public cloud services alongside private data centres. A hybrid multicloud approach brings order to this variety, ensuring that environments work in unison rather than as isolated silos.

Moreover, a hybrid multicloud model supports innovation. Developers gain a consistent platform where applications can be built and deployed across all environments without the need for reconfiguration or additional coding. This seamless compatibility simplifies deployment pipelines, allowing organisations to bring new applications to market faster.

Shifting to hybrid multicloud requires new it thinking

Remember, having multiple clouds doesn't always equal a multicloud approach. Operating a hybrid multicloud model requires a different approach to IT management, one that breaks down traditional silos and introduces new efficiencies. By automating operations across the entire IT landscape, companies can reduce manual oversight and free up valuable time for innovation and strategic projects.

Automation, in this context, is key. By automating routine tasks such as provisioning, monitoring, and resource allocation, organisations can streamline processes and alleviate the burden on IT teams. This, in turn, allows IT teams to refocus on transformative initiatives that drive business growth rather than spending time on day-to-day operations.

For example, a financial services firm could automate data backups and compliance checks across multiple environments, reducing both risk and the workload on IT staff.

Visibility and cost control in a unified operating model

One of the standout benefits of a hybrid multicloud operating model is comprehensive visibility. With a unified platform, businesses gain a panoramic view of their IT landscape—from data centres and private cloud environments to public cloud and edge deployments. This visibility extends not only to infrastructure management

but also to cost control. Enterprises can monitor usage and associated costs across environments, optimising for the best performance-to-cost ratio.

For instance, a healthcare provider might store non-sensitive data on a lower-cost public cloud platform while keeping sensitive patient data on-premises, balancing cost-effectiveness with strict compliance requirements. With centralised visibility, C-level executives have the information needed to make informed decisions, ensuring resources are allocated effectively across all environments.

The path to operational simplicity

Hybrid multicloud as an operating model simplifies IT management by providing a consistent, unified framework. This common model can extend across data centres, public clouds, and edge environments, allowing enterprises to create a single process for deploying, securing, and managing applications across all infrastructures. Additionally, having a standardised framework makes it easier to incorporate AI-driven operations and automation, bolstering the resilience and agility of the entire ecosystem.

The impact of a unified operating model becomes especially apparent when dealing with unexpected demands or crises. A manufacturing company, for instance, could quickly reroute workloads to the cloud if a hardware issue arises on-premises, ensuring continuous operations and preventing downtime.

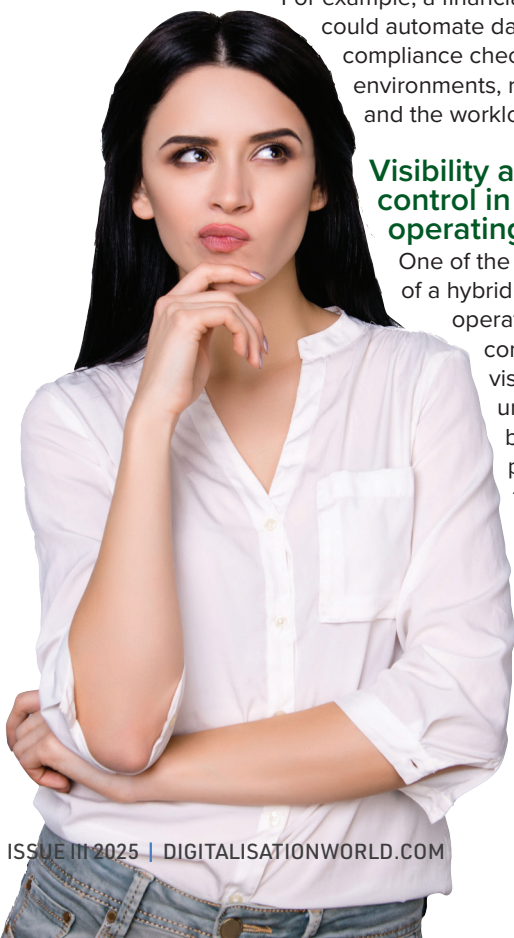
Choosing the right hybrid multicloud platform

The ideal hybrid multicloud platform should offer a comprehensive suite of tools and integrations, providing flexibility and security across the entire IT landscape. Enterprises should look for platforms that align with their existing and future IT goals, enabling them to maximise efficiency while staying adaptable to emerging business requirements. Avoiding vendor lock-in is crucial to ensure adaptability and leverage emerging tools as needs evolve.

For example, a large enterprise might look for a platform that supports a broad range of partnerships and services, ensuring it can leverage the best tools for its industry needs. By investing in the right platform, enterprises can set themselves up for success, creating an agile, resilient infrastructure that drives operational efficiency and cost savings.

A unified approach to modern IT

Ultimately, hybrid multicloud as an operating model is fast becoming a standard, transforming how enterprises manage IT. By treating their diverse environments as a single, adaptive system, businesses can streamline operations, reduce complexity, and unlock new efficiencies. Whether scaling to meet demand, controlling costs, or boosting operational resilience, hybrid multicloud provides the agility and control modern enterprises require.



How evolving businesses can overcome the AI adoption paradox

Artificial Intelligence (AI) stands as one of the most transformative technologies of our era, yet adopting it effectively presents a unique challenge. While 64% of business leaders believe AI can enhance productivity^[1], and over half of IT professionals report accelerated rollouts over the past two years^[2], organisations often stumble at turning enthusiasm into execution.

BY NATHAN MARLOR, GLOBAL HEAD OF DATA AND AI, VERSION 1

THE DILEMMA arises from a cycle of uncertainty: businesses know AI is essential but often lack the skills and strategic clarity to implement it meaningfully. A significant number of small to medium-sized enterprises (43% in the UK) have no concrete AI plans, even when they acknowledge its potential to boost productivity^[3].

Without the right expertise or guidance, this paradox persists, leaving many stuck in a cycle of proofs of concept (PoC) that fail to transition into impactful solutions.

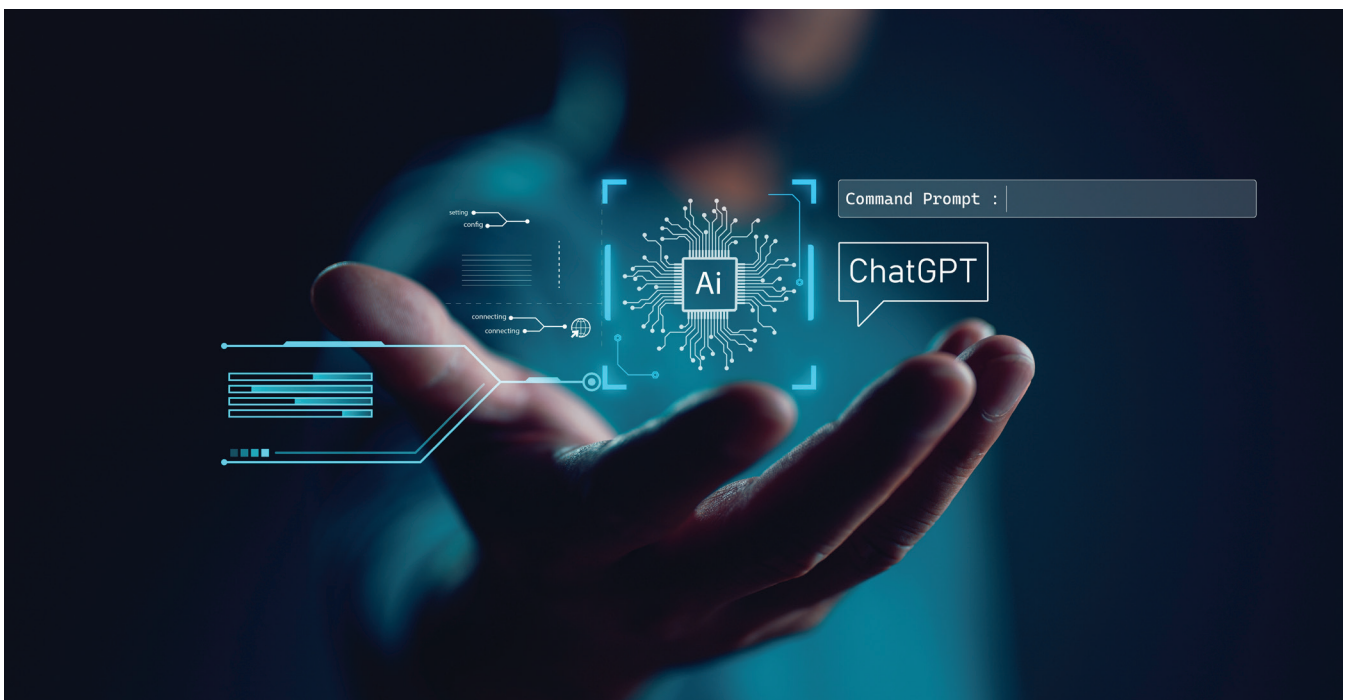
Moreover, the journey from recognising AI's promise to delivering value is hindered by the need to balance limited resources against unclear outcomes.

Organisations must experiment to discover AI's potential benefits but are reluctant to fully commit without first witnessing tangible results. This creates a Catch-22: they need to invest to learn, yet hesitate to invest without guarantees.

Breaking free from this loop demands that businesses view AI as more than just a technology initiative - it must be embedded as a strategic pillar of their future. Overcoming this paradox involves shifting focus from exploration to scalable implementation through three foundational steps.

Breaking the AI Adoption deadlock

To escape the trap of endless pilots and PoCs, organisations must ground their AI efforts in a



AI adoption is not just a technical challenge - it's a cultural one. To break free from the PoC loop, prioritise tools and processes that your teams can embrace and champion

deliberate, actionable framework. This involves addressing three critical dimensions - clarity, readiness, and adoption.

Clarity of purpose: Start with a vision, not an experiment

Most AI initiatives falter because they lack a clear, strategic purpose. Instead of diving into PoCs, begin by defining how AI aligns with your core business objectives.

- **What problem are you solving?** Identify high-impact use cases tied to measurable business outcomes, such as reducing processing times by 30% or enhancing customer satisfaction scores by 20%.
- **What does success look like?** Develop benchmarks and KPIs that signal when an AI initiative has moved beyond experimentation into operational impact.
- **How will it scale?** Ensure the use case is replicable and has a roadmap for expansion. For instance, if a pilot improves customer support in one region, plan how to roll it out globally.

Readiness to execute: Build the right ecosystem

Many organisations stumble into PoC purgatory because they overlook foundational elements needed for execution at scale. Avoid this by assessing and investing in the following:

- **Data infrastructure:** Is your data accessible, clean, and reliable? Fragmented or poor-quality data can doom even the most promising AI projects.
- **Talent and skills:** Address gaps through upskilling, partnerships, or hiring. Ensure teams are equipped not just to implement AI but to maintain and evolve it.
- **Governance:** Establish clear policies to handle compliance, ethical considerations, and risk management early in the project lifecycle.

Adoption at scale: Focus on user-centric solutions

AI adoption is not just a technical challenge - it's a cultural one. To break free from the PoC loop, prioritise tools and processes that your teams can embrace and champion.

- **Engage end-users early:** Collaborate with teams who will use the AI solution daily to refine features and ensure the technology solves their real problems.
- **Simplify deployment:** Use modular or cloud-based AI solutions that are easy to integrate into existing workflows and adaptable to evolving needs.
- **Create an adoption playbook:** Pair technical training with change management strategies. This ensures employees feel confident and motivated to use AI tools effectively.

Remember, successful adoption is less about introducing cutting-edge technology and more about embedding it into the daily rhythm of your business.

Embedding for the long term

The true hallmark of successful AI adoption lies not in isolated projects but in its seamless integration into the core of an organisation's strategy and operations. Businesses must move beyond experimentation, embedding AI as a catalyst for transformation and continuous growth.

Achieving this requires more than technology—it demands a deliberate synthesis of vision, infrastructure, and culture. AI initiatives thrive when they are underpinned by:

- **Purposeful alignment:** Every AI deployment should map directly to strategic objectives, ensuring it drives measurable outcomes that matter to the organisation.
- **Scalable foundations:** Robust systems, adaptable governance, and an eye on future growth create the conditions for AI to evolve from niche applications to enterprise-wide impact.
- **Cultural adoption:** AI succeeds not through imposition but through adoption, where teams see its value in their day-to-day work and embrace its potential to enhance decision-making and efficiency.

The shift from pilot projects to enterprise integration demands a commitment to structured growth, learning, and iteration. Organisations that approach AI with this mindset will not only resolve the adoption paradox but will unlock its potential as a force for sustained competitive advantage in an intelligent, data-driven future.

FURTHER READING / REFERENCE

- [1] Forbes Advisor Survey, April 2024; <https://www.forbes.com/advisor/business/software/ai-in-business/>
- [2] IBM Global AI Adoption Index – Enterprise Report, November 2023; <https://technologymagazine.com/articles/ibm-report-early-adopters-driving-enterprise-ai-adoption>
- [3] British Chambers Of Commerce Employment Trends Report 2024; https://www.britishchambers.org.uk/wp-content/uploads/2024/07/BCC_PERTEMPS_REPORT_FINAL.pdf

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





The hidden costs of legacy systems: why mid-market supply chains need modernising in 2025 and beyond

Mid-market supply chain companies around the world lack the resources required to thrive and adapt in today's fast-paced digital world. Despite this, 97% of supply chain professionals recognise the urgent need to modernise their IT infrastructure, acknowledging that the current systems are inadequate for meeting the needs of modern supply chains. With many companies still relying on legacy technology, some of which are over 20 years old, integration issues are profoundly prominent for both suppliers and customers – this needs to change.

BY SIDDHESH PARAB, SOLUTION ARCHITECT - MANUFACTURING AND SUPPLY CHAIN, PERCIPERE



IN AN ERA where disruptions like port strikes or labour shortages are becoming increasingly more pervasive, heavy reliance on manual systems is no longer sufficient for effective supply chain management and business continuity. Consequently, transformative solutions including enterprise resource planning (ERP) modernisation, shopfloor automation, and warehouse automation solutions have been in greater demand.

Embracing these advancements has become a necessity for mid-market companies that wish to remain resilient and competitive amid evolving challenges within the industry.

The creation of disparate systems

Without the bespoke advancements that modern technology brings, current legacy methods are creating disparate systems brought on by tools

reliant on manual processes. These challenges include the following:

- **Operational inefficiencies:** Legacy ERP and customer relationship management (CRM) tools require manually inputting, storing and extracting data in systems like Excel spreads, increasing the risk of human error. Additionally, this dependency demands significant time and effort to maintain and keep track of such data.
- **Maintenance costs:** Legacy systems are expensive to maintain, making them cost burdens to mid-market companies. Additionally, due to a lack of resources available, legacy systems are often difficult to repair.
- **Security risks:** In order for supply chains to run smoothly, regular software updates are integral. With this in mind, mid-market companies that use legacy systems are much more vulnerable to cyber attacks, data breaches and other security threats because the systems are unable to support new updates.
- **Scalability issues:** With the growth of complex, modern digital operations, legacy systems often struggle to adapt to new technologies, meaning mid-market companies are more likely to fall behind competitors due to incompatibility and inflexibility issues which lead to missed opportunities.
- **Limited visibility:** Real-time visibility is a key driver in ensuring smooth operations within logistics and warehouse management. Unlike modern technology, legacy technology is unable to provide visibility on operations, meaning issues like delays and inventor discrepancies are likely to occur.

Building resilient supply chains

Mid-market supply chain companies that still run core processes on siloed, legacy systems lack the clear, structured foundation that is essential for effective digitisation.

Ultimately, building smart, resilient supply chains requires a shift to intelligent workflows, powered by artificial intelligence (AI) and machine learning (ML). These solutions have the potential to predict demand and supply needs while also being able to automate workflow efficiency.

Modern advanced solutions: seamless collaboration

The first step in moving from a fragmented, transactional set of systems to proven, modern advanced solutions is through the seamless integration of automation technologies directly into core systems like ERP.

These tools revolutionise operations by improving collaboration across the supply chain, ensuring a unified way of working, and alleviating any supply chain issues by strategically upgrading or replacing legacy systems. Other benefits include the following:

- **Enhanced handling:** Intelligent solutions empower warehouse management teams to



efficiently handle all inbound logistics. This includes the inward of materials from external suppliers, internal transfers or customer returns and the handling of units.

- **Scalable cloud infrastructure:** Cloud platforms are preferred for ambitious mid-market organisations because they are a highly scalable and modular approach that supports growth. Instead of engaging in complex capability expansion projects, cloud-based solutions allow businesses to adjust capacity based on their needs.
- **Optimised production:** A manufacturing execution system (MES) supports efficient, more transparent production management, enabling swift resolution of quality and productivity issues quickly while reducing warranty and liability risk.

AI: driving operational efficiency

Additionally, the implementation of AI-driven technologies such as automated bots and operational assisting mechanisms can transform supply chain management. The benefit of adopting such technology is that it reduces errors, improves scalability and enhances operational speed due to a reduction in manual intervention.

These tools can help streamline workflows and reduce manual intervention, helping mid-market companies improve productivity without the requirement of huge upfront costs. Overall, this makes the transition from legacy systems to modern technology and intelligent workflows not only impactful but also cost-effective.

With this approach, mid-market companies can modernise their systems, ensuring AI capabilities are bundled directly into core ERP and CRM packages, allowing them to face evolving challenges head-on.

Why are companies leaving the cloud?

Over the last year or so, the future of hyperscale cloud has been hot on the IT agenda. Having dominated the infrastructure world for the past decade, and pulling in record profits, the undisputed reign of hyperscale cloud is coming into question.

BY ISAAC DOUGLAS, CRO, SERVERS.COM



MANY ORGANIZATIONS are seeking to exit, motivated by unmet expectations including spiraling costs, limited support, increasingly unmanageable complexity, security concerns and an overall lack of control. Some issues are more pertinent than others, but what's clear is that companies are seeking out alternative solutions that mean a partial, if not total, shift away from hyperscale cloud.

As businesses weigh up the benefits of on-prem, colo and infrastructure as a service deployments and especially hybrid architectures, what are the reasons for their hyperscale cloud exit?

Unexpected costs

The escalating costs associated with hyperscale cloud certainly made headlines in 2024. It's understandable then that a lack of transparency

when it comes to infrastructure costs is one of the biggest issues faced by businesses today. In fact, 42% of businesses using hyperscale cloud struggle to predict their monthly cloud bill, 28% have received an unexpectedly large bill for cloud services, and 82% end up wasting more than 10% of their overall cloud spend on hyperscale infrastructure.

For many, it all starts from a seemingly innocent choice made at the very beginning of a company's cloud journey. To get customers signed up, hyperscale cloud providers offer difficult-to-refuse free credits that allow a company to get up and running quickly. Soon enough a business is designing its entire IT infrastructure around a hyperscaler's specific, proprietary products.

Problems arise when the free credits run out and the bills start. Customers are left unable to migrate to more cost-effective solutions without completely rearchitecting or re-engineering. And many IT managers don't have experience carrying out migration projects of this type.

On top of that comes the need for extra security and support from the cloud giant, which sit on a seemingly endless sliding scale of usage-based costs. Cloud resource usage optimization can help, but ultimately businesses are still confronted with growing fees. As recent examples show, the most significant savings are to be had by either integrating alternative sources of compute or migrating away from hyperscale cloud completely.

Security concerns

Public hyperscale cloud environments are prime targets for security challenges, so it is unsurprising to know that 61% of businesses experienced a cloud security incident in 2024. Worryingly, 21% of which resulted in a data breach.



It was only in January 2024 that we saw a major data leak in Microsoft Azure which left hundreds of executive accounts compromised, and up to 97,000 Microsoft Exchange servers vulnerable to attack. It's one of many examples that have influenced companies to manage their own infrastructure, data and security protocols, particularly for organizations dealing with sensitive data.

The inherent security risks brought by public cloud are a product of its shared responsibility model. In these environments, there is always a risk that another business residing on an organization's server will make a security-compromising mistake. And because most data breaches result from human error not hardware failure, the risk is always present. 33% of organizations cite security issues as their primary motivation for leaving the public cloud. And, given that sharing hardware leaves businesses vulnerable to the mistakes of others, mitigating these security risks by leaving public cloud environments seems like a natural step.

A lack of control, and dwindling support

Many assume that the prestige of a big-name cloud label brings excellent levels of support, but for many organizations, this couldn't be further from the truth. In reality, there are negligible levels of support for those only paying the minimum subscription fee, with personalized one on one help available only to those paying premiums on top of an already hefty bill. A problem may be big for a business, but if it isn't critical for your cloud supplier, it's unlikely to be addressed with any urgency.

Break-fix-only support is standard, and in most cases, comes via a link to a generic knowledge base article. Little support for when things go wrong, paired with the fact a business has limited control over its public cloud environment, means serious ramifications can be on the cards. Whilst going on-prem doesn't fix the support issue, it does mean a business will have complete control over managing and troubleshooting its technology, providing it's got a specialized team.

That said, for businesses wanting the support of a hosting provider, there are good hyperscale cloud alternatives out there that offer tailored and reliable support. Including the option for bare metal server hosting, with specialised providers able to personally work with businesses to overcome challenges in real time.

Application-specific requirements

Many organizations assume that public hyperscale cloud environments are a fix-all to every type of workload. The reality is, this perception has been born out of clever marketing campaigns, and not all applications are best suited to the cloud. For example, hyperscale cloud products have been designed for modern applications and many enterprise workloads that currently sit in the cloud

Many organizations assume that public hyperscale cloud environments are a fix-all to every type of workload. The reality is, this perception has been born out of clever marketing campaigns, and not all applications are best suited to the cloud

should probably never have been put there in the first place.

A few years ago, when cloud adoption was the hottest trend in IT, it wasn't unusual to see enterprises move their legacy applications to the cloud en masse. What these companies failed to realize was that these legacy applications weren't set up to benefit from the features offered by hyperscale cloud environments, like containerization and Kubernetes. What was left in the shadows were businesses subject to inefficiencies, increased costs and reduced performance over time - the result of incompatibilities between their applications and their hyperscale cloud environment.

The lesson here for all businesses is that unless there is a real need to refactor applications for the cloud, chances are they're going to be better off being run on dedicated servers instead.

Going all in - is it the only choice?

Many businesses are realizing that a nuanced, flexible approach to infrastructure is the winning formula, with many avoiding the pitfalls of overinvesting in a single technology. As a result, we're seeing hybrid infrastructure deployments becoming increasingly commonplace. Complex, diverse workloads need hybrid IT models to support, blending the best of compute and storage in hyperscale cloud whilst also utilizing on-premises and colocation deployments.

Public cloud isn't a panacea, but instead a technology that can be an incredibly effective tool when used in the right circumstances. Making infrastructure choices on a workload-specific basis enables organizations to optimize performance, cost and increase redundancy by avoiding the single point of failure by going all-in on public hyperscale cloud.

Cloud certainly serves a purpose, but the way businesses have historically been pushed towards cloud services has been inefficient and ineffective. With a renewed, nuanced approach to infrastructure, businesses are moving their technology back on-prem, into colocation or hosted with an IaaS provider with great success. But for most, it means adopting a hybrid approach that combines the best compute types for each workload.

Worldwide security spending to increase by 12.2%

According to the latest forecast from the International Data Corporation (IDC) Worldwide Security Spending Guide, global security spending is expected to grow by 12.2% year on year in 2025.

THE INCREASING complexity and frequency of cyberthreats — accelerated by generative AI (GenAI) and AI in general — are driving organizations worldwide to adopt more advanced defensive measures. As a result, security spending is expected to see sustained growth throughout the 2023–2028 forecast period, reaching \$377 billion in 2028. The United States and Western Europe will continue to account for more than 70% of global security spending in 2025. However, all geographic regions are expected to see consistent growth in security spending this year, with the highest increases in Latin America, Central & Eastern Europe, and the Middle East & Africa.

“Growing digital transformation and hiking emerging technology adoption across the Middle East & Africa (MEA) region — especially countries in the Gulf Cooperation Council (GCC) — have pushed the demand significantly for security solutions to face the evolving threat landscapes. MEA is witnessing substantial investments from both government and enterprises to fight rising cyber threats, with strong awareness for the importance of cybersecurity education and training programs to fortify organizations against possible attacks,” says Eman Elshewy, senior research manager with IDC Data and Analytics.

Security software will be the largest technology group in 2025, representing more than half of the worldwide security market this year, as well as the fastest growing one, with a 14.4% year-on-year

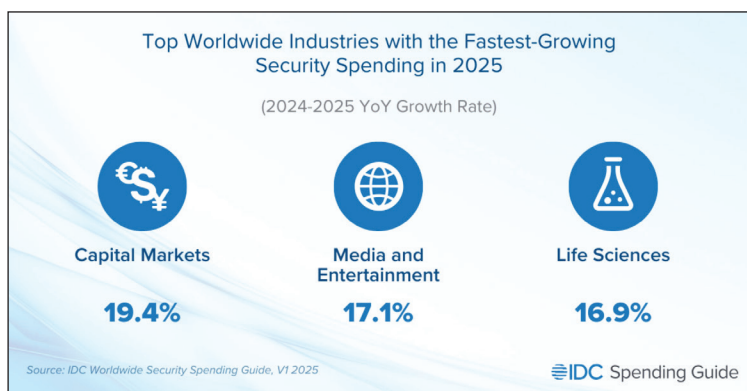
growth rate. The security software market growth will be driven especially by cloud native application protection platform (CNAPP), identity and access management software, and security analytics software growth, reflecting the special focus that companies will put on integrated cyberthreats detection and response around their whole organizational perimeter.

Security services will be the second fastest growing technology group in 2025, driven by the continuous expansion of managed security services, on which organizations of all sizes will continue to increase their focus as a flexible and efficient way to face new security challenges. Finally, security hardware will rank third, achieving single-digit but steady growth in 2025.

Banking, federal/central government, telecommunications, capital markets, and healthcare provider will be the industries spending the most at the global level on security in 2025, while the fastest-growing will be capital markets, media and entertainment, and life sciences with an expected year-on-year growth rate of 19.4%, 17.1%, and 16.9%, respectively in 2025.

“The protection from cyber threats — now enhanced by AI and GenAI — is becoming an increasingly strategic issue for organizations in all industries, especially for those managing critical infrastructures (e.g., oil & gas, telecommunications), developing critical assets (e.g., aerospace & defense, life sciences), or providing key services to clients (e.g., banking, capital markets) and citizens (e.g., federal/central government, healthcare provider),” says Stefano Perini, research manager with IDC Data and Analytics.

“Although national and international regulations still play an important role in guiding organizations’ security strategies — especially in regulated industries — more of them are realizing that having a proactive approach to security is crucial, not only as a short-term operational protection measure but also as a competitive advantage in the long term.”



While large and very large businesses account for the majority of security spending across all regions, small and medium-sized businesses will continue to increase their investments in security throughout the forecast period to address security gaps and protect their assets and processes as their digital transformation accelerates.

Worldwide server market revenue increased 91%

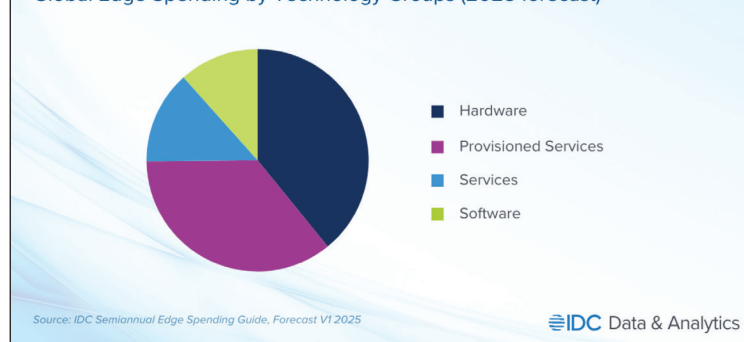
According to the International Data Corporation (IDC) Worldwide Quarterly Server Tracker, the server market reached a record \$77.3 billion dollars in revenue during the last quarter of the year. This quarter showed the second highest growth rate since 2019 with a year-over-year increase of 91% in vendor revenue.

Revenue generated from x86 servers increased 59.9% in 2024Q4 to \$54.8 billion while Non-x86 servers increased 262.1% year over year to \$22.5 billion.

Revenue for servers with an embedded GPU in the fourth quarter of 2024 grew 192.6% year-over-year and for the full year 2024, more than half of the server market revenue came from servers with an embedded GPU. Nvidia continues dominating the server GPU space with over 90% of the total shipments with and embedded GPU in 2024Q4. The fast pace at which hyperscalers and cloud service providers have been adopting servers with embedded GPUs has fueled the server market growth which has more than doubled in size since 2020 with revenue of \$235.7 billion dollars for the full year 2024.

“IDC expects AI adoption to continue growing at a remarkable pace as hyperscalers, CSPs, private companies, and governments around the world

Global Edge Spending by Technology Groups (2025 forecast)



are increasingly prioritizing those investments,” said Lidice Fernandez, group vice president, Worldwide Enterprise Infrastructure Trackers. “Growing concerns around energy consumption for server infrastructure will become a factor in datacenters looking for alternatives to optimize their architectures and minimize energy use.”

Server regional market results

The United States is the second fastest growing region in the server market just behind Canada with an increase of 118.4% compared to the last quarter of 2023, but USA revenues represent 56% of the total revenue in 2024Q4 while Canada accounts for only 1.1% of total revenue globally. China is also growing at a faster rate than other regions with 93.3% year-over-year growth in 2024Q4 and accounting for almost a quarter of the quarterly revenue worldwide.

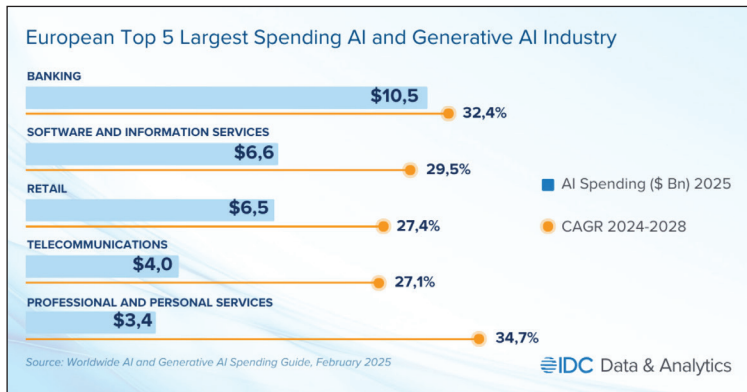
Japan, APeJC and EMEA had double-digit growth this quarter with 66.9%, 43.8% and 28.2% respectively. Latin America 2024Q4 growth was 7%. Overall Server Market Standings, by Company Dell Technologies and Supermicro ended 2024Q4 in a statistical tie* for the number one position with 7.2% and 6.5% revenue share, respectively. Both

Top 5 Companies, Worldwide Server Market, Fourth Quarter of 2024

(Vendor Revenue in US\$ millions)

Company	4Q24 Vendor Revenue	4Q24 Market Share	4Q23 Vendor Revenue	4Q23 Market Share	4Q24/4Q23 Revenue Growth
T1. Dell Technologies*	\$5,540.4	7.2%	\$4,592.6	11.3%	20.6%
T1. Super Micro*	\$5,005.1	6.5%	\$3,230.1	8.0%	55.0%
T2. Hewlett Packard Enterprise*	\$4,239.1	5.5%	\$2,749.2	6.8%	54.2%
T2. IEIT Systems*	\$3,878.1	5.0%	\$2,333.6	5.8%	66.2%
T2. Lenovo*	\$3,783.7	4.9%	\$2,226.1	5.5%	70.0%
ODM Direct	\$36,570.2	47.3%	\$14,313.1	35.4%	155.5%
Rest of Market	\$18,304.6	23.7%	\$11,035.9	27.3%	65.9%
Total	\$77,321.1	100.0%	\$40,480.6	100.0%	91.0%

Source: IDC Worldwide Quarterly Server Tracker, March 13, 2025.



companies had double-digit growth in revenue with Dell Technologies increasing 20.6% year-over-year while Supermicro was up 55% year over year. The next three companies Hewlett Packard Enterprise, IEIT Systems and Lenovo, are statistically tied* for the second position in the market, with shares between 5.5% and 4.9%.

The ODM Direct group of vendors accounted for 47.3% of total revenue in 2024Q4 an increase of 155.5% year over year to \$36.57 billion dollars.

Global spending on edge computing to grow at 13.8%

The International Data Corporation (IDC) has released its latest forecast for Worldwide Edge Computing Spending Guide, featuring a new enterprise industry taxonomy. The newly added structure now includes 27 industries, providing a more detailed and nuanced segmentation by region and country across key manufacturing sectors such as automotive, industrial, consumer packaged goods, life sciences, high-tech and electronics, and aerospace. According to IDC, global spending on edge computing solutions accounts for nearly \$261 Billion in 2025 and is projected to grow at a compound annual growth rate (CAGR) of 13.8%, reaching \$380 Billion by 2028.

“Most industries benefit from the ability to process data closer to the source, leading to faster decision-making, improved security, and cost savings. Retail, industrial manufacturing, life sciences and electronics, healthcare, and life sciences are among the industries that require a particular understanding of their processes and investment behavior,” said Alexandra Rotaru, data & analytics manager at IDC’s Data & Analytics Group. A granular view into these industries will support technology vendors better tailoring their solutions to meet the specific needs and challenges of each industry. This targeted approach enables the delivery of more relevant and effective solutions, ultimately driving growth and innovation in the edge computing landscape.”

IDC segments edge spending for more than 1000 named enterprise use cases related to six enterprise domains: AI, IoT, AR, VR, Drones, and Robotics, unlocking significant opportunities across various

industries. Augmented Reality, followed by Artificial Intelligence, are the fastest growing segments over the forecast period, driving increased investments in key sectors.

In 2025, Retail & Services sector accounts for the largest share of investments in edge solutions, representing nearly 28% of total global spending. In this sector, use cases such as video analytics, dynamic real-time carrier performance and optimized operations account for the biggest spending. The Manufacturing & Resources sector follows as the second largest, collectively making up a quarter of worldwide spending. Additionally, financial services are projected to experience the fastest growth in spending over the next five years, with a compound annual growth rate (CAGR) exceeding 15%, driven by spending related to Augmented Fraud Analysis and Investigation use case in the AI domain.

The Edge Spending Guide also forecasts infrastructure investments made by Service Providers to deliver services to enterprises in the form of multi-access edge computing (MEC), content delivery networks, and virtual network functions, and are forecasted to reach almost \$100 billion by 2028.

“Edge computing is poised to redefine how businesses leverage real-time data, and its future hinges on tailored, industry-specific solutions that address unique operational demands,” said Dave McCarthy, research vice president, Cloud and Edge Services at IDC. “We’re seeing service providers double down on investments—building out low-latency networks, enhancing AI-driven edge analytics, and forging partnerships to deliver scalable, secure infrastructure. These efforts are critical to realizing the full potential of edge computing, enabling everything from smarter manufacturing floors to responsive healthcare systems, and ultimately driving a new wave of innovation across verticals.”

Regarding technology spending, Hardware is the most significant investment at the beginning of the forecast, driven by the rapidly deploying AI accelerated processors. This evolution is fueled by the increasing demand for real-time data processing and the proliferation of intelligent end points that increasingly require edge-based compute, storage and network capabilities such as those supporting agentic AI capabilities. However, aggregate Services segments (includes Provisioned and Professional Services) are estimated to surpass the hardware share by 2028, posting a five-year CAGR of more than 18%. Within Provisioned Services, infrastructure as a service (IaaS) remains the fastest-growing category driven by the need for scalable, flexible, and cost-effective solutions that can handle the growing computational demands of AI workloads.

From a geographic perspective, North America will remain the edge spending leader throughout the

forecast period, followed by Western Europe and China. Western Europe, China and Latin America will experience the fastest spending growth over the five-year forecast.

European AI spending to reach \$144 billion

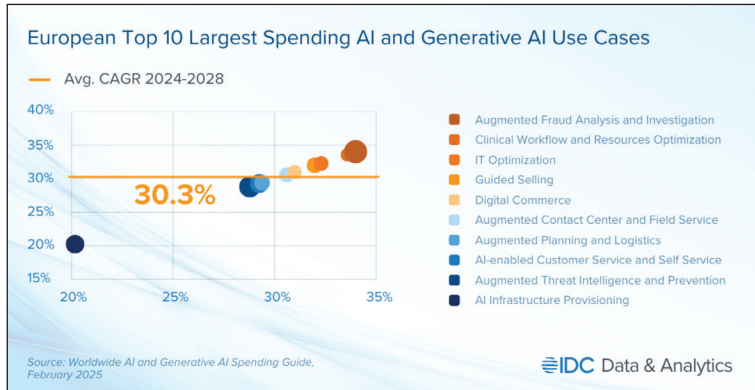
According to a new forecast from the International Data Corporation (IDC) Worldwide AI and Generative AI Spending Guide, European spending in artificial intelligence will reach \$144.6 billion in 2028, based on a compound annual growth rate (CAGR) of 30.3% over the 2024-2028 forecast period.

Generative AI (GenAI) is gaining momentum in Europe, currently accounting for nearly a fourth of the total AI market. By 2028, its share is expected to grow to one-third. According to IDC's 2024 Industry IT & Communications Survey, 87% of European companies plan to allocate up to 30% of their total AI budget to GenAI solutions. "Generative AI is increasingly requiring more coordinated efforts to be deployed company wide," says Carla La Croce, research manager, Data and Analytics at IDC. "GenAI is a top priority for C-suite leaders and opens opportunities to develop more integrated internal strategies among C-suites."

Software remains the leading technology segment of artificial intelligence spending, accounting for more than 60% of total AI and GenAI market, of which 44% is represented by AI platforms, that facilitate the development of AI models and applications. Software is also the fastest-growing technology segment (33.5% 2024-2028 CAGR, with AI platforms growing well above the average) followed by services (27.2% 2024-2028 CAGR) and hardware (24.7% 2024-2028 CAGR). Hardware and services account for a similar share throughout the period, but servers exhibited higher-than-expected growth in 2024, driven by investment by hyperscalers and services providers.

From an industry perspective, the financial services sector is expected to spend the most proportionally on AI solutions (23% of the market in 2025), with banking at the forefront. Strategic digital investments of European banks are aimed at enhancing efficiency, strengthening risk management, and ensuring long-term profitability, and AI specifically provides opportunities to enhance customer experience and improve cybersecurity and consumer protection. Indeed, the biggest use cases in this industry are related to augmented fraud analysis and investigation, augmented threat intelligence and prevention, augmented contact center and field service, and AI-enabled customer service and self service, always with a focus on IT optimization.

The second largest industry for AI spending is software and information services, where key investments are made for AI infrastructure provisioning, which accounts for more than half of



the total spending in this industry. The third biggest industry is retail. Despite economic pressure and unstable consumer sentiment in Europe, AI and GenAI are significantly transforming the European retail sector by enhancing customer experiences with more personalized shopping, and also optimizing operations, and driving sales. Digital commerce is the leading use case, accounting for a third of the market, followed by AI-enabled customer service and self service and augmented planning and logistics.]

In terms of the fastest growing industries, media and entertainment are leading the way, each with CAGRs exceeding 35% over the 2024-2028 period, driven by the increasing adoption of GenAI solutions for content creation and personalization or video production.

Professional and personal services is likewise expected to also grow well above the average, along with healthcare and life sciences. Leading use cases in healthcare are clinical workflow and resources optimization, and augmented pharmaceutical research and discovery in life sciences.

IDC expects significant investments in security and customer-focused areas, from augmented fraud analysis and investigation and augmented threat intelligence and prevention to AI-enabled customer service and self-service, which are more cross-industries applications, but also in AI infrastructure provisioning, which is instead driven by specific industries' spending (software and information services, telco and retail) in servers.

Another interesting perspective that the Worldwide AI and Generative AI Spending Guide provides is the functional use cases view, which shows where AI and GenAI are used the most across functions. In 2025, customer service, IT operations, AI infrastructure provisioning, and sales are the areas where AI and GenAI are most frequently applied.

Functional areas that start from a smaller investment base but are expected to show higher than average growth include human resources, engineering R&D, and marketing.

Keep IT cool in the era of AI

EcoStruxure IT Design CFD by Schneider Electric helps you design efficient, optimally-cooled data centers

Optimizing cooling and energy consumption requires an understanding of airflow patterns in the data center whitespace, which can only be predicted by and visualized with the science of computational fluid dynamics (CFD).

Now, for the first time, the technology Schneider Electric uses to design robust and efficient data centers is available to everyone.

- Physics-based predictive analyses
- Follows ASHRAE guidelines for data center modeling
- Designed for any skill level, from salespeople to consulting engineers
- Browser-based technology, with no special hardware requirements
- High-accuracy analyses delivered in seconds or minutes, not hours
- Supported by 20+ years of research and dozens of patents and technical publications

Equipment Models – Easily choose from a range of data center equipment models from racks, to coolers, to floor tiles.

IT Airflow Effectiveness and Cooler Airflow Efficiency – Industry-leading metrics guide you to optimize airflow.

Cooling Analysis Report – Generate a comprehensive report of your data center with one click.

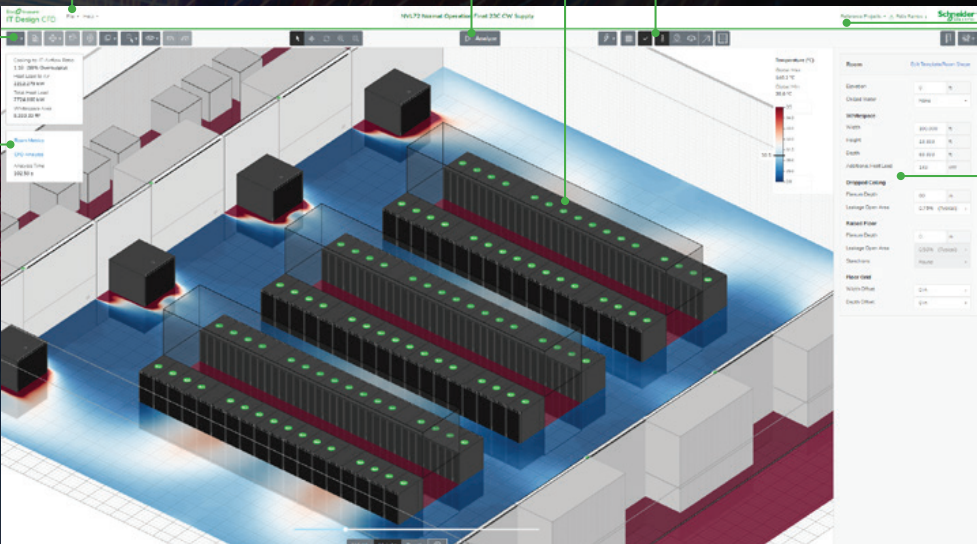
CFD Analysis – The fastest full-physics solver in the industry delivering results in seconds or minutes, not hours.

Cooling Check – At-a-glance performance of all IT racks and coolers.

Visualization Planes and Streamlines – Visualize airflow patterns, temperatures and more.

Reference Designs – Quickly start your design from pre-built templates.

Room and Equipment Attributes – Intuitive settings for key room and equipment properties.



Explore

www.se.com/uk