DW DIGITALISATION WORLD

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

ISSUE VIII 2024

DIGITALISATIONWORLD.COM

WHY THE UK'S CYBER SECURITY AND RESILIENCE BILL MAKES A CYBER SECURITY 'TRIPLE PLAY' ESSENTIAL

DW talks to
Eric Herzog

INFINIDAT

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

AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

APC™

40Years

Make greater

IMPACT

with an industry-leading network

Celebrate 40 years with APC.

Start leveraging four decades of uninterrupted protection, connectivity, and unparalleled reliability with the APC UPS family, a legacy marked by pioneering UPS technology and an unwavering commitment to innovation.

https://www.apc.com/uk/en/product-category/88972-uninterruptible-power-supply-ups/

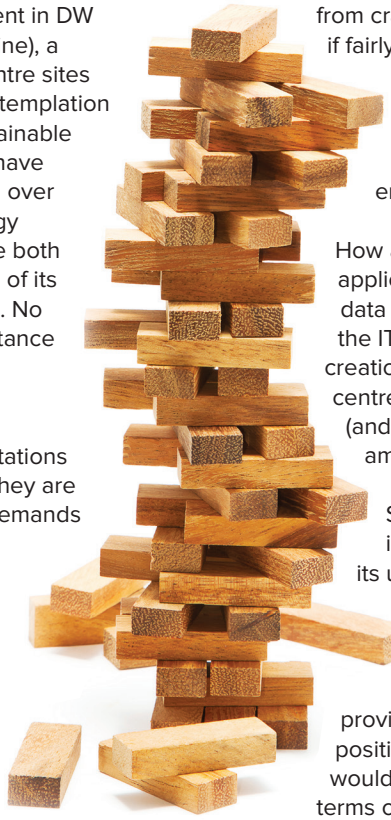
Life Is On Schneider Electric

VIEWPOINT

By Phil Alsop, Editor

An (impossibly) complicated balancing act?

FOLLOWING ON from my comment in DW Issue 6 (Issue 7 is a video magazine), a couple of recent visits to data centre sites have only served to add to the daily contemplation I tend to give to the ongoing digital/sustainable debate. In both cases, the data centres have been massively upgraded and improved over a number of years in terms of their energy efficiency. As an aside, the work they are both doing is, put simply, astonishing in terms of its contribution to human life into the future. No hyperbole, just a statement of the importance of the work being enabled by the IT kit housed in the data centres.



As part of both visits, there were presentations looking at the future of data centres as they are required to cope with the high density demands of AI computing workloads. There's no disguising the fact that, in the short term at least, data centre power consumption is set to increase significantly.

However, once the LLMs have done all of the number crunching, there's every chance that the myriad of AI applications which come online in the medium to long term future will enable all manner of activities which will be saving substantial amounts of energy, compared to what was done previously. And then there are the applications that were talked about on the data centre visits. The contribution that AI can make to the future of human health, for example, is almost limitless (provided we think that extending human life every upwards is a good thing!).

I guess the real challenge lies in trying to calculate the overall environmental impact of any specific activity, from cradle to grave. Scopes 1-3 are a valiant, if fairly crude, attempt to do this. What's needed is a much more (AI-powered?!) granular calculator, which can take account of every single aspect of an activity in terms of its net impact on the environment.

How and where the energy required for the application was generated and brought to the data centre; the manufacture and journey of the IT hardware to the facility; the software creation cycle; the humans required in the data centre – how they travel to and from work (and much, much more at the micro level I am sure.

Set against this is the (hopefully) positive impact the application provides to its users and the world in general. Take a video meeting application, for example. Just how many journeys do video calls save, set against the environmental impact of their provision? One imagines there's a major positive at the end of this calculation, but it would be good to know exactly how much in terms of sustainability as opposed to having a gut feeling that good is being done.

And, as already stated, the calculation needs to be comprehensive – not capable of being used and abused to conveniently leave out environmental harms along the way, to generate a falsely positive end result.

The Environmental Impact Calculator – let's hope we will all be able to use one soon to understand how our activities impact the planet – for good and bad.

CONTENTS

ISSUE VIII 2024

DW DIGITALISATION WORLD

NEWS

DIGITALISATION WORLD

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

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

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

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

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

Angel BUSINESS COMMUNICATIONS

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.

ISSN 2396-9016 (Online)

Modernisation challenges hinder IT team productivity

While modernisation challenges impact productivity and business success, survey finds that all IT decision makers are turning to experienced partners for support.

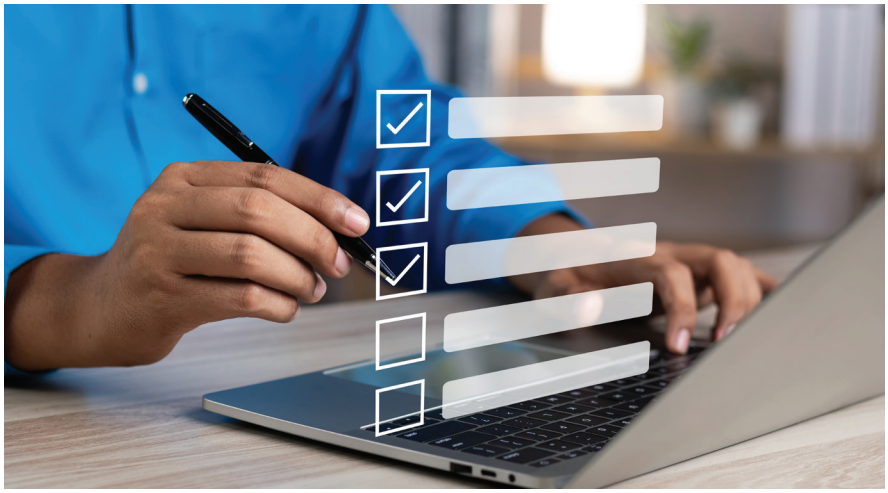
ROCKET SOFTWARE has published the findings from its survey, IT Modernisation Without Disruption. Rocket Software commissioned Forrester Consulting in this survey of over 300 global decision makers, including CIOs, VPs and Directors, responsible for modernising their company's IT environment to explore strategies and the value external partners provided.

Key survey findings include:

- Modernisation challenges are disruptive to businesses, with one-third (33%) of respondents reporting that these roadblocks led to reduced productivity
- Successful IT modernisation strategies are tied to both stronger technological and business outcomes, which is why many C-suite executives (42%) are championing these efforts, recognising their t transformative potential

For businesses, modernisation is not just about staying relevant; it's essential for staying agile and competitive. The key to successful transformation is how an organisation strategically aligns their technology to their business and the context it operates in, whether that be healthcare, financial services, manufacturing or retail. Though it can be daunting, businesses are not backing down. Sixty-nine (69%) percent of respondents believe IT modernisation is crucial for achieving their business goals over the next 12 months.

However, these modernisation journeys are not without roadblocks. Modernisation challenges include costly and time-consuming application re-write projects, with over half of respondents (51%) attempting at least six re-write projects as part of their cloud migration strategy due to multiple failures. Rewriting applications can



be a costly mistake for businesses, as it often leads to extended timelines, operational disruptions, and frequently fails to deliver the expected outcomes. Challenges also include concerns over security (41%), talent shortages/ skills gap (38%), and inadequate tools (30%). These challenges are negatively impacting business – 38% said modernisation challenges have hurt their ability to recruit new talent, 35% stated that these challenges reduce their ability to compete, and 44% said that these obstacles have led to delayed timelines. However, the survey found that organisations who work with external partners (e.g., hyperscalers, managed service providers, trusted software vendors, system integrators, or external consultants) to supplement internal shortcomings reduce these modernisation challenges.

"Modernisation is an imperative for achieving both business and technology goals, yet it comes with a range of challenges," said Phil Buckellew, President, Infrastructure Modernisation Business Unit, at Rocket Software. "At Rocket Software, we are committed to supporting enterprises through this complex process, ensuring that modernisation is seamless and effective. We recognise that modernisation goes beyond technology upgrades - it involves a strategic transformation of an organisation's entire operation. Our focus is on enhancing efficiency, improving customer experiences, and driving competitive innovation. The key to a successful modernisation journey is partnering with a team that not only understands the intricacies of the process but also provides the solutions, expertise and personalised support to meet you at every stage of your journey."

The survey found that priorities differ for organisations at different points in their modernisation journeys. Fifty one (51%) percent of respondents who have been on their IT modernising journey for more than one year selected "improved ability to take advantage of cloud-native, scalable applications" as a top desired outcome, compared to only 37% of those who are just starting out. Experienced IT modernisation decision makers were also more likely to select "competitive parity or advantage" as a top outcome compared to beginners. These insights demonstrate how those with greater maturity are making IT modernisation a more strategic advantage for their business.

Ransomware surge demands coordinated global response

Amid intensifying geopolitical tensions, ransomware attacks in 2024 are set to reach record levels, escalating the risks faced by companies worldwide

THERE IS A SHIFT toward more sophisticated extortion tactics, emphasizing the urgent need for coordinated global action and robust incident response strategies as organizations confront increasingly aggressive and persistent cyber threats, says GlobalData, a leading data and analytics company. Globaldata's latest Thematic Intelligence report, "Deep Dive into Ransomware," reveals that 2023 was the third worst year on record for ransom attacks and the worst for payments, which reached over $1 billion, citing Chainalysis.

David Bicknell, Principal Analyst of Thematic Intelligence at GlobalData, comments: "Companies are under constant threat from ransomware attacks and, once breached, must decide whether to pay the ransom to recover their operations and data. The surge in attacks reflects a shift toward a more aggressive ransomware landscape. What began as phishing-led incursions requiring decryption keys has evolved into sophisticated extortion, where attackers post victims' data on the dark web, leading to further attacks by other groups."

Companies that have suffered ransomware attacks include Boeing, Caesars Entertainment, MGM Resorts, Change Healthcare, Royal Mail, Johnson Controls, the UK's National Health Service (NHS), Sony, Capita, and Dish Network.

Jordan Strzelecki, Associate Analyst of Thematic Intelligence at GlobalData, adds: "High-profile law enforcement takedowns are increasingly disrupting ransomware gangs. Successful action against Hive, LockBit, and AlphV temporarily stemmed the tide of attacks and sent a warning to cybercriminals

that their days could be numbered. "However, the ransomware industry is never static, and new gangs continually emerge to replace those that have been taken down or have become less effective. Gang affiliates are taking a larger slice of ransom payments and are making repeat attacks. Ransomware gangs are now actively competing to attract talent."

Preparedness pays off

THE COMMVAULT SURVEY, done in collaboration with GigaOm, shows that organisations that have endured cyber incidents in the past don't want to get burned again. Consequently, they often reassess and invest in cyber resilience and recovery strategies in very meaningful ways.

According to the survey:

- **Investments in cyber resilience increase:** Organisations that have been breached spend nearly 30% more on cybersecurity measures than those that haven't.
- **More attention is given to understanding data risk profiles:** Breached organisations are nearly 2.5 times more likely to prioritise understanding their data risk profiles, which highlight data types and relative levels of risk.
- **Cyber readiness testing is prioritised:** Breached organisations conduct more testing to find gaps in their cyber preparedness plans. Twenty percent of organisations that haven't been breached do not test their recovery plan at all, that number drops to just 2% for organisations that have been breached.

The impact of these added investments and focus on cyber resilience is significant. According to the survey, breached organisations that have invested in comprehensive cyber recovery plans recover 41% faster than their less-prepared counterparts.

In terms of specific recovery times, breached organisations state that they are 32% more likely to recover within 48 hours compared to those that have not been breached – a much better outcome than the recovery times noted by other respondents, which could be three weeks or more. This reduced downtime can translate to significant savings, both in terms of direct financial losses and the preservation of customer trust and brand reputation.

Much like health insurance, where the cost of coverage often far outweighs the potential expenses of medical emergencies, cyber recovery readiness serves a similar purpose.

The report underscores that the costs of being breached – ranging from operational disruption to regulatory fines – far exceed the expenses of proactive cyber resilience measures. were able to recover data and resume normal operations.

Lack of data quality and governance seen as major AI obstacles

Data integrity study from Precisely and Drexel University's LeBow College of Business exposes widespread data trust issues and its impact on data and AI initiatives.

PRECISELY has released a new study conducted in collaboration with the Center for Applied AI and Business Analytics at Drexel University's LeBow College of Business (Drexel LeBow). Key findings from this year's 2025 Outlook: Data Integrity Trends and Insights1 report shed light on the most pressing challenges businesses face in achieving AI readiness and other data initiatives, and how they're prioritising investments in data integrity to overcome them.

The report reveals that, despite 60 percent of organisations stating AI is a key influence on data programmes (a 46 percent increase from 2023), only 12 percent report that their data is of sufficient quality and accessibility for effective AI implementation. For years, companies have grappled with poor-quality data, leading to a deeply rooted distrust in the data used for analytics and AI. While 76 percent of organisations say data-driven decision-making is a top goal for their data programmes, 67 percent still don't completely trust the data they rely on for these decisions, a rise from 55 percent in 2023.

A lack of data governance is the primary data challenge inhibiting AI initiatives, cited by 62 percent of organisations. This is likely due to the role that data governance programmes play in managing an organisation's data usage – including where it's stored, its lineage, who has access to it, whether it has personally identifiable information (PII) attributes, and more.

Skills gap further impede AI adoption
With more companies prioritising data-driven decision-making, the shortage of skills and resources needed for data management, analytics, and AI has also grown this year. Forty-two percent (42 percent) say a shortage of

skills and resources continues to be one of their biggest challenges to data programmes, up from 37 percent in 2023.

"While organisations are eager to benefit from AI's capabilities, a talent shortfall impedes AI integration," said Murugan Anandarajan, PhD, professor and academic director at the Center for Applied AI and Business Analytics at Drexel University's LeBow College of Business. "Our research findings highlight that gap, with 60 percent of respondents citing a lack of AI skills and training as a significant challenge in launching AI initiatives – a signal to business leaders that upskilling must be a strategic imperative."

Data quality remains the top data integrity challenge and priority
Given the findings relating to AI, it's unsurprising to see data quality reported as a primary focus for organisations worldwide. This year, 64 percent of respondents identified data quality as their top data integrity challenge, up from 50 percent in 2023. Additionally, the overall perceptions of data quality have declined, with 77 percent of respondents rating the quality of their data as average or worse, compared to 66 percent in the previous year.

The most significant barrier to achieving high-quality data is the lack of adequate tools for automating data quality processes, cited by 49 percent of respondents. Inconsistent data definitions and formats (45 percent), and data volume (43 percent) are also top concerns.

The research also shows that poor data quality continues to have a ripple effect across all aspects of data integrity, with 50 percent of respondents reporting that data quality is the number one issue impacting their organisation's data integration projects.
Data governance adoption has risen dramatically
To combat challenges with data trust, quality, and AI success, organisations are increasingly realising the importance of robust data governance programmes. This year, 51 percent of organisations identified data governance as a top challenge to data integrity, second only to data quality, marking a dramatic 89 percent increase from the previous year (up from 27 percent in 2023). In line with this, adoption has increased with 71 percent reporting that their organisation has a data governance programme, compared to 60 percent in 2023.

This increased investment is paying off. Organisations that invested in data governance programmes report benefiting from improved data quality (58 percent), improved quality of data analytics and insights (58 percent), increased collaboration (57 percent), increased regulatory compliance (50 percent) and faster access to relevant data (36 percent).

The 2023 report predicted the emergence of data enrichment and spatial analytics as business-critical technologies, and this year's report demonstrates a significant leap forward in adoption. In 2024, 28 percent report data enrichment as a priority for data integrity, up from 23 percent in 2023.

Survey reveals AI's real-world priorities

Domino Data Lab has published the findings of a survey conducted by BARC it commissioned of 278 enterprise AI leaders globally about how their companies are deploying AI in the real world, the support they get, and their leading concerns.

THE RESULTS SHOW that while GenAI may be stoking AI enthusiasm and even budgets, today's real-world AI initiatives and their underlying stacks are still diverse, rapidly evolving, and far from perfect for addressing today's infrastructure and governance challenges.

Key findings include:

21% of enterprises have a blank cheque from their board for all types of AI, with 72% saying they have sufficient budget.
While GenAI gets all the attention, slightly more companies are getting predictive AI into production (53%), indicating that traditional machine learning is still the workhorse.
More than 90% of enterprises plan to make some infrastructure adjustments to account for their GenAI journey, most commonly using updated versions of their pre-GenAI stacks.

Everyone needs to upgrade AI governance: 95% face a governance remodel or reboot to update their frameworks and processes for today's modern model landscape.
Not many companies are hindered by compute scarcity, with 9 out of 10 saying it's not impacting their needs, and most (87%) are confident in leveraging their AI stacks across various vendor silicon and infrastructure.
When it comes to enterprise attitudes on AI, one thing is for sure: corporate boards are all-in. The survey revealed that 21% of enterprises have a blank cheque from the board for all types of AI. Additionally, nearly all boards are paying attention to AI. Only 5% of respondents said their board hadn't engaged or set a strategy on AI, and 72% reported their boards provided sufficient support for all AI, including GenAI.

However, the research revealed that some boards may be overly excited by GenAI. A third (34%) of respondents said GenAI initiatives get more board support than they deserve, depriving support from other forms of AI. 8% said it was difficult to get funding for anything other than GenAI.
While attitudes are solid and often very focused on pushing GenAI, actions are more varied. Companies are rapidly putting GenAI into production, but more traditional forms of AI and data analytics remain the workhorse. Slightly more companies, 53% and 57% respectively, are putting predictive AI — i.e. machine learning — and advanced analytics projects into production than GenAI (49%). However, the distinction between these types of projects is blurring. 41% of leaders say that they have projects that use both predictive and generative AI in production.

This survey also found that enterprises are still early in their AI journeys.
Over half of respondents are still in the planning, researching, or proof of concept stage when it comes to GenAI, and 47% have not yet put predictive AI projects into production even though these technologies have been available for decades — an indication that companies still struggle to move from experimentation phases to productising all types of AI.

As GenAI reshapes the AI landscape, enterprises in EMEA are taking a more cautious and measured approach, reflecting unique regional challenges and regulatory considerations.

Respondents in EMEA are nearly twice as likely (47%) than their North American counterparts (31%) to keep their existing AI stack as a result of GenAI's arrival. Perhaps this is because EMEA AI Leaders were less likely to rate their boards' support for all AI as sufficient (66% of EMEA respondents vs. 77% of North American respondents).
If companies are indeed amidst a rapid AI deployment spree, then this comes with the need for robust governance frameworks and scalable infrastructure to support these advanced technologies. The study found that 95% face a governance remodel or reboot to update their frameworks and processes for today's modern model landscape.
Reassuringly, most companies say they have a baseline of necessary responsible AI infrastructure and processes in place. They believe that they can incorporate more data sources and more data into the AI equation.

Most (65%) of the respondents said their companies need only add new processes to existing governance frameworks to compensate for this change. Also, in a possible reaction by companies now subject to the new EU AI Act, nearly double the percentage of EMEA respondents (16%) indicated that they would fully replace their current governance framework in the era of GenAI, compared to just 9% of respondents in North America.

Organisations value ESG as highly as security and cloud migration projects

Despite a tough economic climate, sustainability remains a crucial focus, particularly when selecting a cloud provider.

86% of businesses report that environmental, social and governance (ESG) and sustainability is important to their organisation when deciding which cloud vendor to work with, with almost half (44%) considering it extremely important.

This second figure is up from 30% in 2023, indicating that despite media reports of ESG being put on the backburner by many companies, they remain committed to continued sustainability efforts. This is according to research conducted by the Cloud Industry Forum.

The data from this year's report indicates that organisations value ESG highly, with 40% of respondents reporting that IT sustainability is an important project for their organisation. This ranks equally with other areas of business such as security and cloud migration, and is second only to artificial intelligence (42%).

Despite this, when deciding on whether or not to work with a cloud service provider, cost is still king, being the most important priority for 45% of respondents. Next, 41% referenced the availability of services and 39% mentioned partnering with a trustworthy company as being key factors, all ranking more highly than sustainability credentials (28%).

However, the research also found that 49% of organisations said they would always reject a prospective vendor if they gave a poor response on their ESG and sustainability strategy.

This continued emphasis on sustainability is supported by the finding that 79% of organisations are now measuring the carbon footprint of their existing data storage infrastructure in the cloud.

According to the data, 47% of organisations have already been measuring this for more than 12 months, and just 7% indicated that they do not have any plans to measure this in the future.

Further, organisations are taking crucial steps to reach net zero despite economic constraints, with 87% of organisations planning to reach net zero by at least 2050. More than a quarter (26%) of respondents plan to achieve the milestone before 2030.

On the whole, businesses are largely positive about their sustainability credentials, and this is growing year on year. 31% of respondents now believe the sustainability of their organisation's IT emissions is 'established and mature', a figure that has increased from 16% in 2023.

David Terrar, CEO of the Cloud Industry Forum, said: "Despite recent media reports suggesting that organisations are watering down ESG commitments amid a difficult economic climate, this year's data shows that the focus on sustainability continues to grow.

"Cost undoubtedly – and understandably – remains a key factor for all businesses, but it doesn't come at the expense of sustainability. Businesses are continuing to invest time, effort and funds into ESG initiatives and are set to continue to do so.

"It's also positive to see that businesses are taking steps to measure the carbon footprint of their storage infrastructure. The recent AI boom has been met with some opposition due to the energy intensiveness of popular tools such as large language models, so it's important that businesses are taking steps to measure and combat this as the use of these tools grows.

"Cloud service providers should take note that a large proportion of businesses are prepared to reject partnerships on the basis of sustainability alone, and should ensure they are setting themselves high standards in this area. Those companies able to demonstrate clear consideration of sustainability issues will stand ahead of those relying on the prospect of cost savings alone."

Hybrid apps and AI drive sevenfold increase in organisations' digital maturity levels

F5's 2024 Digital Enterprise Maturity Index finds that more than a quarter of organisations are now classed as digitally mature.

DIGITAL TRANSFORMATION has accelerated markedly over the last year, with a sevenfold increase in organisations ranked at the highest level of digital maturity, new research from F5 shows. For F5's second Digital Enterprise Maturity Index (DEMI) report1, 713 responses from the 2024 State of Application Strategy Report were assessed against a set of six core technical capabilities2: infrastructure, app delivery, data, Site Reliability Engineering (SRE) operations, observability and automation, and security.

This year, 29% of organisations qualified as "doers" and were deemed to be making significant strides forward in their digital transformation efforts. In the 2023 report, only 4% reached this level. 54% of organisations surveyed in 2024 were classified as "dabblers", and just 17% were deemed digital "dawdlers".

In 2024, digital maturity was particularly evident in the hybrid and distributed nature of organisation's infrastructure, system automation levels, and how effectively data is managed and stored to make it observable.

82% of "doers" are operating hybrid apps with components in at least two distinct environments, indicating advanced digital readiness and effective AI integration. This was the case for 51% of "dabblers" and 10% of "dawdlers". Furthermore, 59% of "doers" have also automated systems that can execute scripts based on conditions and push delivery and security policies. By contrast, only 37% of "dabblers" and 16% of "dawdlers" were operating in this way.

The DEMI Report also found that 74% of "doers" have automated their network security and 53% have done so for network infrastructure, compared to just 8% and 4% of "dawdlers", respectively.

"Digitally mature organisations are increasingly defined by flexible infrastructures that stretch across core, cloud and edge locations," said Lori MacVittie, Chief Evangelist and Distinguished Engineer at F5. "That means tackling the complexity introduced by different frameworks, as well as APIs and consoles. It is encouraging that this year's 'doers' are rising to the challenge, investing in hybrid apps that allow them to optimise deployment for both performance and cost. This is also a key indicator of AI readiness."

The growing influence of GenAI
Fundamental to that AI readiness is the observability of data – the raw material for AI models – and the ability to make it operational. According to this year's DEMI report, 94% of "doers" are either maintaining multiple data stores or consolidating into a single data lake. Meanwhile, two-thirds (65%) of "dawdlers" said they had no strategy for data observability.
The use of Site Reliability Engineering (SRE) practices, which underpins the deployment of hybrid apps, was another sign of digital maturity and AI readiness.

Almost all "doers" (97%) have adopted or are planning to adopt an SRE approach, whereas the vast majority (86%) of "dawdlers" are not.
SRE operations fundamentally operate on a different set of principles that emphasise achieving business outcomes rather than avoiding operational incidents. That means implementing practices that support reducing mean time to resolution (MTTR) and availability of services, rather than trying to hit an unattainable uptime metric.

This year, there was a strong correlation between organisations using SRE

and those able to deploy hybrid applications, scale AI-driven operations and maintain performance. The DEMI report also noted that "doers" managed an average of 468 APIs, once again highlighting a sophisticated digital infrastructure prepared for AI integration.

Another key trend from this year's data showed that there was a significant gap between the most and least digitally mature companies when it comes to security. "Doers" not only implemented more robust security measures but were also more confident in their ability to repel threats.

When it came to the implementation of SDLC (secure development lifecycle), which integrates security into the development of software before the first line of code is written, "doers" scored 13.5/15, compared to 10/15 for "dabblers", and 5.5/15 for "dawdlers". Similar scores were recorded for the adoption of zero trust security policies. Fueled by a growing reliance on AI, 92% of mature organisations said they have adopted zero trust principles, reflecting higher confidence levels in their security frameworks.

On a scale of 1-5, "doers" who had implemented zero trust said they were very confident (4.4/5) about their ability to repeal an application or API layer attack. "Dabblers" and "dawdlers" rated themselves 2.8/5 and 2.2/5 respectively.

Malwarebytes releases "ThreatDown 2024 State of Ransomware" report

Manufacturing has become a default target with a 71% year-on-year increase in attacks.

MALWAREBYTES has released its "ThreatDown 2024 State of Ransomware" report. The comprehensive report reveals an alarming increase in ransomware attacks over the past year, alongside significant shifts in the tactics and strategies employed by cybercriminals that underscore the necessity for organisations to implement around-the-clock monitoring and investigation of suspicious behaviors.

As the corporate product portfolio of Malwarebytes, ThreatDown solutions are purpose-built to overpower threats, while empowering IT, through easy-to-use, effective technologies such as Endpoint Detection & Response (EDR) and Managed Detection & Response (MDR).

"Ransomware gangs have time and motivation on their side. They constantly evolve to respond to the latest technologies chasing at their tails," said Marcin Kleczynski, Founder and CEO, Malwarebytes. "We've seen this very distinctly over the past year as widespread adoption of technologies like EDR has helped identify attackers before they launch malware, pushing ransomware gangs to work more quickly and put more effort into hiding themselves.

Organisations and MSPs need additional support and continuous coverage to outmanoeuvre today's criminals."

Report Key Findings:

- The US experienced a dramatic 63% increase in ransomware attacks, with the UK seeing an even greater rise of 67%.
- The share of attacks carried out by gangs outside the top 15 increased from 25% to 31%, indicating that ransomware is becoming more accessible to a broader range of cybercriminals.
- The US accounts for 48% of all ransomware attacks worldwide but suffers 60% of the world's attacks on education and 71% of attacks on healthcare.

The manufacturing sector saw a staggering 71% year-on-year increase in ransomware attacks, highlighting the need for robust cybersecurity measures in this rapidly digitising industry.

Top Three Ransomware Trends

The report also features insights from the ThreatDown MDR team on three key shifts in the tactics and techniques of ransomware gangs:

- **Living off the Land (LOTL) Techniques:** Ransomware gangs are increasingly relying on built-in system administration tools to carry out their attacks, making detection and prevention more challenging for teams without a dedicated Security Operations Center (SOC).
- **Nighttime Attacks:** Most ransomware attacks now occur between 1 a.m. and 5 a.m., targeting organizations when IT staff are less likely to be present.
- **Faster Attack Timelines:** The entire ransomware attack chain, from initial access to data encryption, has reduced from weeks to mere hours, necessitating rapid detection and response capabilities.

"The question I ask organisations is do you have someone prepared to stop an attack at 2 a.m. on a Sunday with your existing technology stack and staff resources?" said Chris Kissel, Research Vice President, Security & Trust, IDC."

MANAGED SERVICES SUMMIT

MANCHESTER

19 NOVEMBER 2024

MANCHESTER CENTRAL

ENJOYING its 5th year, the Managed Services Summit Manchester builds on the successes of previous years as well as its sister events in London and Amsterdam, which are firmly established as the leading managed services events for the UK and European IT channel.

Featuring conference session presentations by major industry speakers, the Summit will also provide opportune networking breaks for delegates to meet with potential business partners.

The unique mix of high-level presentations plus the ability to explore and debate the most pressing business issues with sponsors and peers across the industry, makes this a must-attend event for any senior decision maker in the IT channel.

If you want to be the complete MSP for your clients and are unsure who to partner with to achieve this, then register now for MSS Manchester, it could be the most important event you attend this year.

THEMES, TOPICS & TRENDS

The Managed Services Summit will address the key trends and issues that impact the managed services sector including:

- How to build differentiation within an increasingly competitive market
- Emerging advances in AI, automation and XaaS
- Maximise value and increase efficiencies for MSPs and their customers
- Increasing knowledge of new technologies, processes, and best practice
- Analysing trends in buyer behaviour and successful sales strategies
- Changes and trends in regulatory compliance
- Successfully adoption of Zero Trust Architecture (ZTA)
- The state of cloud adoption, and hybrid and edge computing
- Hybrid and remote working best practice
- Addressing the growing cyber security skills gap
- Participation with local business community leadership organisations

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Angel BUSINESS COMMUNICATIONS

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

IT EUROPA

Stephen Osborne
stephen.osborne@iteuropa.com
+44 (0)7516 502689

Aadil Shah
aadil.shah@iteuropa.com
+44 (0)7516 501193

manchester.managedservicessummit.com

ANGEL EVENTS

Gartner predicts 40% of Generative AI solutions will be multimodal by 2027

Forty percent of generative AI (GenAI) solutions will be multimodal (text, image, audio and video) by 2027, up from 1% in 2023, according to Gartner, Inc. This shift from individual to multimodal models provides an enhanced human-AI interaction and an opportunity for GenAI-enabled offerings to be differentiated.

SPEAKING AT Gartner IT Symposium/Xpo on the Gold Coast today, Erick Brethenoux, Distinguished VP Analyst at Gartner, said, "As the GenAI market evolves towards models natively trained on more than one modality, this helps capture relationships between different data streams and has the potential to scale the benefits of GenAI across all data types and applications. It also allows AI to support humans in performing more tasks, regardless of the environment."

Multimodal GenAI is one of two technologies identified in the 2024 Gartner Hype Cycle for Generative AI, where early adoption has potential to lead to notable competitive advantage and time-to-market benefits. Along with open-source large language models (LLMs), both technologies have high impact potential on organizations within the next five years.

Among the GenAI innovations Gartner expects will reach mainstream adoption within 10 years, two technologies have been identified as offering the highest potential - domain-specific GenAI models and autonomous agents (see Figure 1).

"Navigating the GenAI ecosystem will continue to be overwhelming for enterprises due to a chaotic and fast-moving ecosystem of technologies and vendors," said Arun Chandrasekaran, Distinguished VP Analyst at Gartner. "GenAI is in the Trough of Disillusionment with the beginning of industry consolidation. Real benefits will emerge once the hype subsides, with advances in capabilities likely to come at a rapid pace over the next few years."

Multimodal GenAI

Multimodal GenAI will have a transformational impact on enterprise applications by enabling the addition of new features and functionality otherwise unachievable. The impact is not limited to specific industries or use cases, and can be applied at any touchpoint between AI and humans. Today, many multimodal models are limited to two or three modalities, though this will increase over the next few years to include more.

"In the real world, people encounter and comprehend information through a combination of different modalities such as audio, visual and sensing," said Brethenoux. "Multimodal GenAI is important because data is typically multimodal. When single modality models are combined or assembled to support multimodal GenAI applications, it often leads to latency and less accurate results, resulting in a lower quality experience."

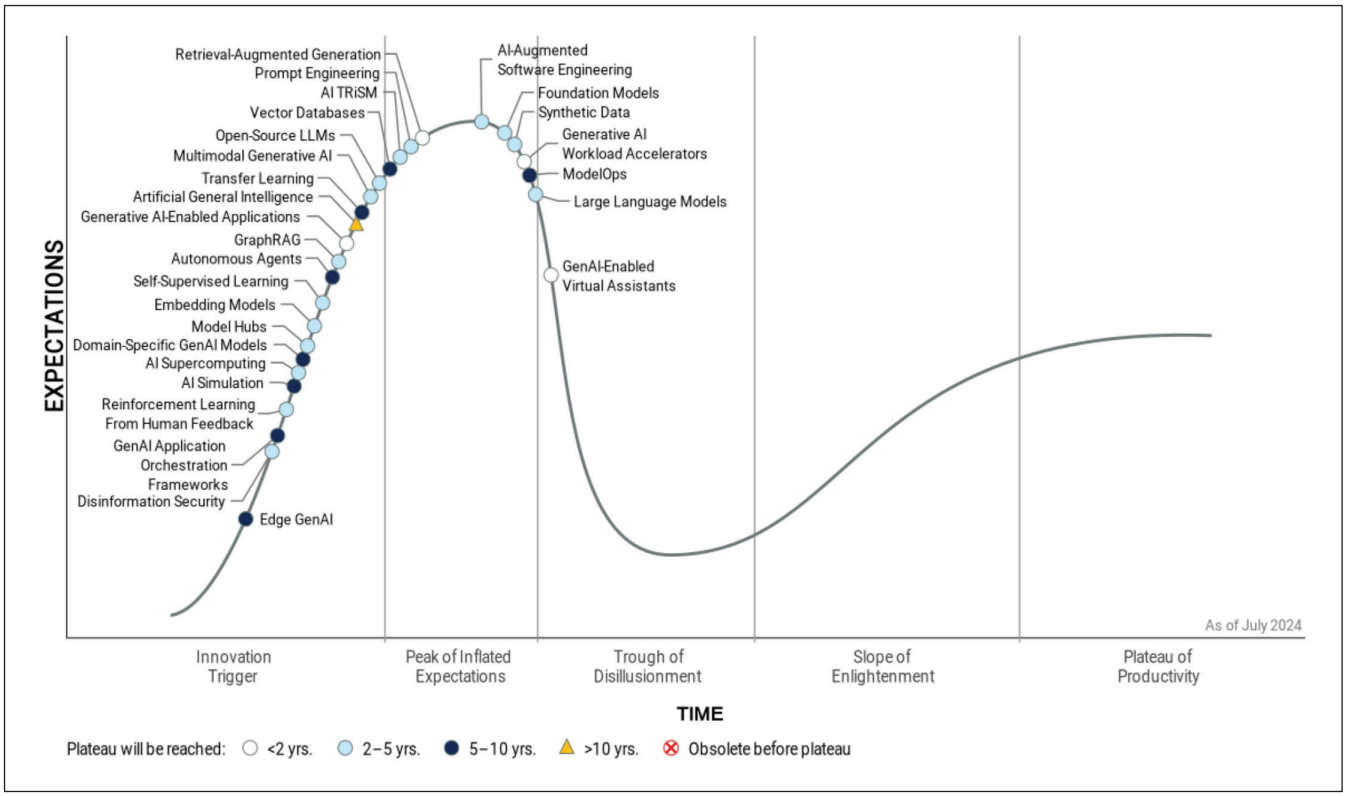
Open-source LLMs

Open-source LLMs are deep-learning foundation models that accelerate enterprise value from the implementation of GenAI, by democratizing commercial access and allowing developers to optimize models for specific tasks and use cases. Additionally, they provide access to developer communities in enterprises, academia and other research roles that are working toward common goals to improve and make the models more valuable.

"Open-source LLMs increase innovation potential through customization, better control over privacy and security, model transparency, ability to leverage collaborative development, and potential to reduce vendor lock-in," said Chandrasekaran. "Ultimately, they offer enterprises smaller models that are easier and less costly to train, and enable business applications and core business processes."

Domain-specific GenAI models

Domain-specific GenAI models are optimized for the needs of specific industries, business functions or tasks. They can improve use-case alignment within the enterprise, while delivering improved accuracy, security and privacy, as well as better contextualized answers. This reduces the need for advanced prompt engineering compared with general-purpose models and can lower hallucination risks through targeted training.



➤ Figure 1: Hype Cycle for Generative AI, 2024. Source: Gartner (September 2024)

"Domain-specific models can achieve faster time to value, improved performance and enhanced security for AI projects by providing a more advanced starting point for industry-specific tasks," said Chandrasekaran. "This will encourage broader adoption of GenAI because organizations will be able to apply them to use cases where general-purpose models are not performant enough."

Autonomous agents

Autonomous agents are combined systems that achieve defined goals without human intervention. They use a variety of AI techniques to identify patterns in their environment, make decisions, invoke a sequence of actions and generate outputs. These agents have the potential to learn from their environment and improve over time, enabling them to handle complex tasks.

"Autonomous agents represent a significant shift in AI capabilities," said Brethenoux. "Their independent operation and decision capabilities enable them to improve business operations, enhance customer experiences and enable new products and services.

This will likely deliver cost savings, granting a competitive edge. It also poses an organizational workforce shift from delivery to supervision."

Global information security spending to grow 15% in 2025

Worldwide end-user spending on information security is projected to total $212 billion in 2025, an increase of 15.1% from 2024, according to a new forecast from Gartner, Inc. In 2024, global information security end-user spending is estimated to reach $183.9 billion.

"The continued heightened threat environment, cloud movement and talent crunch are pushing security to the top of the priorities list and pressing chief information security officers (CISOs) to increase their organization's security spend," said Shailendra Upadhyay, Senior Research Principal at Gartner. "Furthermore, organizations are currently assessing their endpoint protection platform (EPP) and endpoint detection and response (EDR) needs and making adjustments to boost their operational resilience and incident response following the CrowdStrike outage."

The adoption of AI and generative AI (GenAI) continue to increase investments in security software markets like application security, data security and privacy, and infrastructure protection. Through 2025, GenAI will trigger a spike in the cybersecurity resources required to secure it, leading to an expected 15% increase on security software spending (see Table 1).

Since the release of GenAI, attackers are increasingly employing tools along with large language models (LLMs) to carry out large-scale social engineering attacks, and Gartner predicts that by 2027, 17% of total cyberattacks/data leaks will involve generative AI. As organizations continue to move to the cloud, Gartner analysts expect an increase in cloud security solutions, and the market share of cloud-native solutions will grow.

The combined cloud access security brokers (CASB) and cloud workload protection platforms (CWPP) market is estimated to reach $8.7 billion in 2025, up from forecasted $6.7 billion in 2024.

Segment	2023 Spending	2023 Growth (%)	2024 Spending	2024 Growth (%)	2025 Spending	2025 Growth (%)
Security Software	76,574	13.6	87,481	14.2	100,692	15.1
Security Services	65,556	13.6	74,478	13.6	86,073	15.6
Network Security	19,985	6.2	21,912	9.6	24,787	13.1
Total	162,115	12.7	183,872	13.4	211,552	15.1

Source: Gartner (August 2024)

➤ Table 1. Information Security End-User Spending by Segment, Worldwide, 2023-2025 (Millions of U.S. Dollars)

The global skills shortage in the cybersecurity industry is a major factor driving investment in the security services market (security consulting services, security professional services and managed security services) which is expected to grow faster than the other security segments.

Hype Cycle highlights developer productivity, total experience, AI and security

The 25 disruptive technologies to watch on the Gartner, Inc. Hype Cycle for Emerging Technologies, 2024 fall into four key areas: autonomous AI, developer productivity, total experience, and human-centric security and privacy programs.

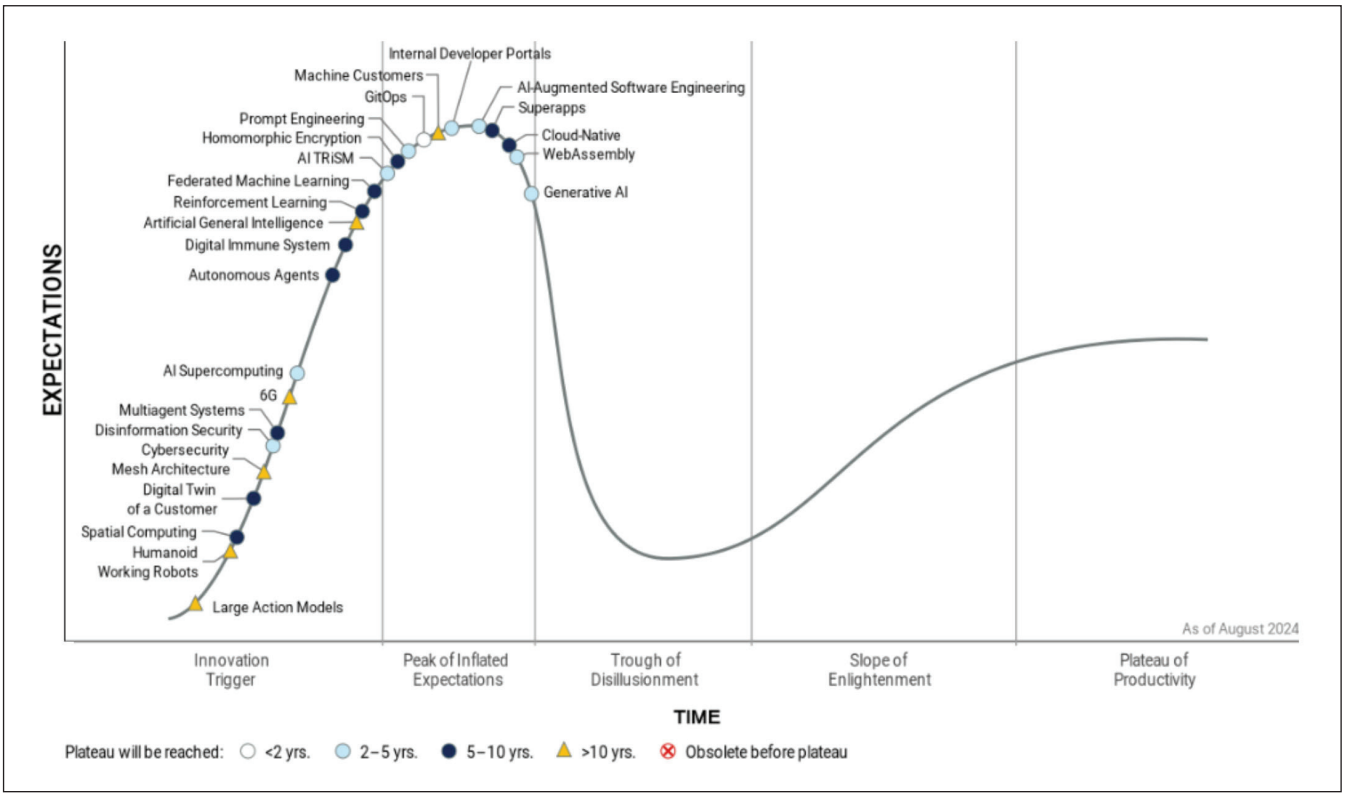
“Generative AI (GenAI) is over the Peak of Inflated Expectations as business focus continues to shift from excitement around foundation models to use cases that drive ROI,” said Arun Chandrasekaran, Distinguished VP Analyst at Gartner.

“This is accelerating autonomous AI. While the current generation of AI models lack agency, AI research labs are rapidly releasing agents which can dynamically interact with their environment to achieve goals, although this development will be a gradual process.

“Even as AI continues to grab the attention, CIOs and other IT executives must also examine other emerging technologies with transformational potential for developers, security and customer and employee experience and strategize how to exploit these technologies in line with their organizations’ ability to handle unproven technologies,” said Chandrasekaran.

The Hype Cycle for Emerging Technologies is unique among Gartner Hype Cycles because it distills key insights from more than 2,000 technologies and applied frameworks that Gartner profiles each year into a succinct set of “must-know” emerging technologies. These technologies have potential to deliver transformational benefits over the next two to 10 years (see Figure 1).

➤ Figure 2: Hype Cycle for Emerging Technologies, 2024. Source: Gartner (August 2024)



Four Themes of Emerging Technology Trends
Autonomous AI: AI's fast evolution is producing autonomous AI systems that can operate with minimal human oversight, improve themselves and become effective at decision-making in complex environments. These advanced AI systems that can perform any task a human can perform are beginning to move slowly from science fiction to reality. These technologies include multiagent systems, large action models, machine customers, humanoid working robots, autonomous agents, and reinforcement learning.

Boost developer

Productivity: Developer productivity is about more than writing code quickly. It's influenced by developers' effective communication and collaboration, and their feeling of energized focus, full involvement and enjoyment (being in the "flow state").

"Technology is revolutionizing the way developers design and deliver software, making them more productive than ever," said Chandrasekaran. "It's ensuring they deliver higher-quality products quickly while maximizing gains by improving developer satisfaction, collaboration, and flow."

Emerging technologies enabling developer productivity include AI-augmented software engineering, cloud-native, GitOps, internal developer portals, prompt engineering and WebAssembly.

Empower With Total Experience: Total experience is a strategy that creates superior shared experiences by intertwining customer experience, employee experience, multiexperience and user experience practices. It uses technology to address critical interactions, empowering both customers and employees, with the goal of driving greater confidence, satisfaction, loyalty and advocacy. Technologies to assess include digital twin of a customer, spatial computing, superapps and 6G.

Deliver Human-Centric Security and Privacy: Organizations will become more resilient by using security and privacy techniques that create a culture of mutual trust and awareness of shared risks between teams.

"Security practices too often rely on the premise that humans can behave in a completely safe and secure way. But when employees must make a choice between security and business delivery, they often choose business delivery, sometimes bypassing too-stringent security controls," said Chandrasekaran. "Human-centric security and privacy weaves a tight security and privacy fabric into the organization's digital design."

Emerging technologies supporting human-centric security and privacy include AI TRiSM, cybersecurity mesh architecture, digital immune system, disinformation security, federated machine learning and homomorphic encryption.

AI to contribute $19.9 trillion to the global Eeconomy through 2030

New research from IDC entitled, The Global Impact of Artificial Intelligence on the Economy and Jobs, predicts that business spending to adopt artificial intelligence (AI), to use AI in existing business operations, and to deliver better products/services to business and consumer customers will have a cumulative global economic impact of $19.9 trillion through 2030 and drive 3.5% of global GDP in 2030.

AS A RESULT, AI will affect jobs across every region of the world, impacting industries like contact center operations, translation, accounting, and machinery inspection. Helping to trigger this shift are business leaders who almost unanimously, 98%, view AI as a priority for their organizations.

AI's net positive global economic impact

According to the research, in 2030, every new dollar spent on business-related AI solutions and services will generate $4.60 into the global economy, in terms of indirect and induced effects. This is determined by:

- Increased spending on AI solutions and services driven by accelerated AI adoption
- Economic stimulus among AI adopters, seeing benefits in terms of increased production and new revenue streams
- Impact along the whole AI providers supply chain, increasing revenue for the providers of essential supplies to AI solutions and services providers

"In 2024, AI entered a phase of accelerated development and deployment defined by widespread integration that's led to a surge in enterprise investments aimed at significantly optimizing operational costs and timelines," said Lapo Fioretti, senior research analyst, Emerging Technologies and Macroeconomics, IDC. "By automating routine tasks and unlocking new efficiencies, AI will have profound economic consequences, reshaping industries, creating new markets, and altering the competitive landscape."

Impact on employment - New roles emerge while others remain resilient

The majority of respondents to IDC's Future of Work Employees Survey expect some (48%) or most (15%) parts of their work to be automated by AI and other tech over the next two years, while only a minority (3%) of employees expect their jobs to be fully automated by AI.

While some work will be negatively impacted by the proliferation of AI, new positions such as AI Ethics Specialists and AI Prompt Engineers will emerge as dedicated roles within global organizations. The research further indicates that a "human touch intensity," combined with the level of "task repetitiveness" by which each job is characterized, will inform organizations about roles that are subject to a full AI and automation replacement, versus those where tech's role will be to augment human capabilities. As such, positions where human social and emotional capabilities are critical, such as nursing and roles where decision-making encompasses ethics and comprehension beyond numbers will remain robust.

"Understandably, we're all curious to know if AI will replace our jobs," said Rick Villars, group vice president, Worldwide Research, IDC. "As a CEO interviewed by IDC's Andrea Siviero said, 'Based on this research it's clear that we should be asking ourselves how our jobs can be made easier

and better by AI. AI will not replace your job but someone who knows how to use AI better than you will.'"

Edge computing spending to reach $378 Billion in 2028

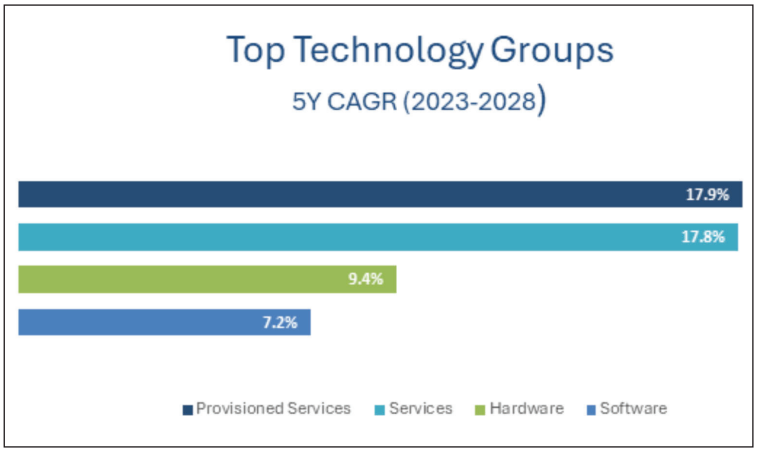
According to the International Data Corporation (IDC) Worldwide Edge Spending Guide, global spending on edge computing is estimated to reach $228 billion in 2024, marking a 14% increase from 2023. This includes combined enterprise and service provider spending on hardware, software, professional services, and provisioned services for edge solutions. The forecast anticipates sustained strong growth through 2028, with spending expected to be near $378 billion, growing at a solid double-digit CAGR.

According to IDC, the edge encompasses the technology-related actions outside of centralized data centers, serving as an intermediary between connected endpoints and the core IT environment. Edge is a crucial technology infrastructure that extends and innovates on the capabilities found in core datacenters, whether enterprise- or service-provider-oriented. The edge ecosystem comprises various technologies and services, including computing infrastructure (such as servers, storage, and networking equipment), diverse software (such as system infrastructure, security, and application development and deployment), as well as professional implementation and management services and provisioned services delivering cloud-based technologies.

"As the focus of AI shifts from training to inference, edge computing will be required to address the need for reduced latency and enhanced privacy," said Dave McCarthy, research vice president, Cloud and Edge Services at IDC. "This trend not only optimizes operation efficiencies but also fosters new business models that were previously not possible with centralized infrastructure. Distributing applications and data to edge locations enables faster decision-making with reduced network congestion."

The IDC Edge Spending Guide segments edge spending for more than 500 named enterprise use cases related to six domains – Artificial Intelligence (AI), Internet of Things (IoT), Augmented Reality (AR), Virtual Reality (VR), Drones, and Robotics – unlocking significant opportunities across various industries.

In manufacturing, accounting for the largest portion of spending, edge enables real-time monitoring of equipment and processes, reducing downtime and improving operational efficiency. Predictive maintenance use case, powered by AI at the edge, helps companies avoid costly breakdowns by identifying issues before they escalate.
In utilities, edge continues to enable smarter, more efficient, and real-time management of critical



infrastructure such as electricity, water, and gas. With the increasing deployment of renewable energy sources, smart grids, and IoT-enabled devices, edge is a critical solution for utilities companies to help with processing vast amounts of data quickly and securely.

Banking is the fastest-growing industry in terms of spending. Driven by the rise of AI-powered services, edge transforms how banks handle data processing, fraud detection, and customer interactions. Examples of use cases include AI-optimized operations, augmented fraud analysis and investigation, and others.
IDC expects all 19 enterprise industries profiled in the spending guide will see five-year double-digit compound annual growth rates (CAGRs) over the forecast period.

However, the service provider segment will see the largest CAGR over the forecast period. In the service provider domain, investments in edge service delivery are built on infrastructure spending for multi-access edge computing (MEC), content delivery networks, and virtual network functions. Multi-access edge computing (MEC) represents the fastest growing area, becoming increasingly critical for supporting the ultra-reliable, low-latency communications required by next-generation applications steered by the widespread of 5G networks, IoT, and artificial intelligence.

"Enterprises are now accelerating their investments in edge and AI to drive real-time analytics, automation, and enhanced customer experiences, particularly in manufacturing, utilities, healthcare, and retail. Key technologies like AI-powered devices, edge servers with GPUs, and 5G connectivity are gaining traction, enabling organizations to process data closer to the source and achieve higher performance," said Alexandra Rotaru, manager, Data & Analytics, Europe. "In this journey, the service providers will play a critical role by offering tailored solutions, from infrastructure deployment to AI integration and edge management, helping enterprises seamlessly adopt edge and AI and unlock its full potential for advanced innovation."

Regarding technology spending, the most significant investment will stay within hardware at the beginning of the forecast, driven by AI processors and accelerators in edge infrastructure systems that are projected to generate increased demand in the coming years. However, provisioned services are estimated to surpass the hardware share by 2028. Within provisioned services, infrastructure as a service will represent the fastest growth category as a great tool that facilitates rapid development, deployment, and iteration of AI models and edge computing applications. Although small in terms of overall spending, on-premises software will remain a critical component of edge infrastructure, driven by accelerated demand for analytics and AI software.

A close-up of a graph description automatically generated

From a geographic perspective, North America will remain the edge spending leader throughout the forecast period, followed by Western Europe, with Germany and the United Kingdom leading the spending. China, Latin America and Asia/Pacfic (excluding Japan and China) will experience the fastest spending growth over the five-year forecast.

UC&C market to grow through 2028

The worldwide unified communications and collaboration (UC&C) market is forecast to reach $69.1 billion in revenue in 2024, an increase of 7.5% compared to 2023, according to a new report from International Data Corporation (IDC). During the 2023-2028 forecast period, the UC&C market is expected to witness a slightly lower compound annual growth rate (CAGR) of 5.7% to reach $85 billion by 2028.

“The UC&C market has matured after significant investments were made in the past few years by businesses to address the changed work environment,” said Jitesh Gera, research manager, Unified Communications and Collaboration at IDC. “In addition, the crowded UC&C market has led many solutions toward commoditization. However, AI is now changing the game altogether, bringing a fresh wave of new and differentiated capabilities that are likely to draw more investments in the coming years as businesses vie for enhanced employee productivity and better customer engagement.”

Among the drivers of UC&C adoption is the continued introduction of artificial intelligence (AI) capabilities into UC&C solutions. This includes AI-enabled videoconferencing and telephony solutions that help improve productivity as well as capabilities that improve business outcomes across employees and customers

Looking across the key technology segments of the UC&C market, the two software segments — UC collaboration (meeting software without voice telephony subscriptions) and unified communications as a service (UCaaS) (meeting software including voice telephony subscriptions) — accounted for most of the worldwide market revenue (89% in 2023). Their share is expected to rise further as growth in the hardware segments (IP telephony and enterprise videoconferencing systems) turns negative over the forecast period. Meanwhile, the UC collaboration segment is forecast to outpace the overall market with a five-year CAGR of 7.6%.

Microsoft continued to lead the worldwide UC&C market with a 44.7% market share by revenue in Q1 2024. Zoom and Cisco followed distantly with a 6.4% and 5.5% market share respectively. The remainder of the market is largely fragmented with several smaller players focused mainly on specific industry verticals or small and medium businesses (SMBs) in their focus geographies.

Among the drivers of UC&C adoption is the continued introduction of artificial intelligence (AI) capabilities into UC&C solutions. This includes AI-enabled videoconferencing and telephony solutions that help improve productivity as well as capabilities that improve business outcomes across employees and customers. IDC also expects cloud-based UC&C deployments will increase over time, replacing on-premises deployments as security and data integrity continue to improve. And the integration of UC solutions with contact center platforms will continue as buyers look to simplify their technology stacks and reduce their administrative load to work with single unified providers of UC, CC, and CPaaS capabilities.

IDC defines unified communications and collaboration (UC&C) as a bundled, integrated UC/UCaaS and UC collaboration solution stack that may include an advanced telephony solution integrated with messaging (i.e., email, voice, and fax), instant messaging (IM) or chat, presence, and conferencing platforms for web conferencing, audioconferencing, and/or videoconferencing. These platforms also typically include the creation of teams/channels for access-based communications and knowledge sharing, plus tools such as digital whiteboards, screen sharing, live polls/surveys, questions and answers (Q&As), and meeting scheduling capabilities. In addition to the software-based platforms facilitating these communications, the UC&C market includes the primary hardware that enables these communications, including desktop IP phones, videoconferencing endpoints comprising integrated camera and microphone systems, and multipoint control units (MCUs) bridging multiple users and devices into a single network. These UC&C solutions can be delivered via on-premises infrastructure or on public/private cloud on an as-a-service basis.

SDC AWARDS 2024

CELEBRATING 15 YEARS OF SUCCESS

33 Categories across 4 Themes

28 NOVEMBER 2024

LEONARDO ROYAL HOTEL LONDON CITY

KEY DATES:

1 NOVEMBER: VOTING CLOSES

28 NOVEMBER: AWARDS CEREMONY

VOTE NOW!

HEADLINE SPONSOR

EXAGRID®

CATEGORY SPONSORS

INFINIDAT ninjaOne Schneider Electric

SPONSORSHIP PACKAGES

The SDC Awards offer extensive branding and sponsorship opportunities. Sponsors are front and centre of the awards marketing program running from now through to the glittering ceremony itself.

Book your Seats/Table NOW!

To reward your team with an evening to remember

Email: awards@sdcawards.com

For sponsorship opportunities and/or to book your awards table please contact:
awards@sdcawards.com or call +44 (0)2476 718970

VOTE HERE: https://sdcawards.com/vote

Angel BUSINESS COMMUNICATIONS

ANGEL EVENTS

Why the UK's Cyber Security and Resilience Bill makes a cyber security 'Triple Play' essential

As a leading provider of enterprise storage solutions, Infinidat takes Cyber Security Awareness Month very seriously. **Eric Herzog, CMO at Infinidat** has been speaking with DW about the company's drive to educate IT and executive leaders, and why new cyber resilience legal requirements mean enterprises need to change the way they approach their storage infrastructure.

OCTOBER is a critical time in the cyber security sector and, timed to coincide with Cyber Security Awareness Month, Infinidat has been working to raise awareness about the critical need for enterprises to increase their cyber storage resilience in the battle against cyber attacks, with next-generation data protection and recovery capabilities.

Across all sectors, Infinidat is seeing a shift in the enterprise market to emphasise the importance of cyber storage resilience and cyber recovery in storage infrastructure, with a special focus on near instantaneous cyber recovery. Years ago, cyber storage resilience was one of the last things discussed in conversations about enterprise storage but is now one of the first things that enterprise IT buyers, including CIOs, CTOs, and CISOs, want to understand thoroughly. Enterprise cyber storage resilience has become 'top-of-mind' from a cyber security standpoint.

Consequently, the timing of Infinidat's efforts on cyber storage education couldn't be more pertinent, given that the UK's new Cyber Security and Resilience Bill is set to become legislation imminently. Over the past 20 months, the UK has experienced a significant increase in serious cyber security incidents, targeting almost every critical sector of the economy, including local government, utilities, healthcare, education, transportation and finance.

In 2023, organisations managing critical IT infrastructure reported more disruptive cyber attacks, with well over 3,285 attacks involving ransomware alone. The same pattern has continued with increasing frequency into 2024. These attacks

have caused chaos, with surgeries postponed, schools needing to close and cancelled train and flight services. Add to this the security and privacy risks of such large-scale data breaches and it's a perfect storm. Cyber criminals have become far more sophisticated and strategic about their attacks. Stronger defences need to be in place across all sectors and cyber resilient storage has emerged as the last line of defence against ransomware and malware.

Protecting data is one of the most critical actions an IT team must do in the data centre today. Expectations for restoring data and backing up data at multi-petabyte scale have changed. IT teams need to increase next-generation data protection capabilities, with data integrity and high reliability with 100% availability, which is what Infinidat provides. Best practices require an enterprise to ensure data validity and near-instantaneous recovery of primary storage and backup repositories, regardless of the size of the dataset. This accelerates digital disaster recovery when a cyber attack happens.

Timely new cyber security legislation

The increased frequency of attacks has resulted in impending changes to the UK's cyber security legislation, with the introduction of a new Cyber Security and Resilience Bill. This bill was announced during the King's Speech in July 2024 and is expected to be introduced into Parliament imminently.

Given that the UK had previously only partially implemented the EU's NIS2 framework, this new law will rigorously strengthen the UK's defences against cyber attacks, particularly in critical national infrastructure like the NHS and government departments. The bill is very timely and responds to the growing cyber threats faced by essential services and the digital economy, as well as recent high-profile incidents that have targeted key sectors including education and transportation hubs. The focus will be on tougher security measures, mandatory vulnerability assessments, and enhanced incident response capabilities.

So how should enterprises approach the greater rigour needed for cyber security solutions in practical terms? What solutions are required and how does this impact storage? We advocate a triple play, with equal emphasis on cyber storage resiliency, detection and recovery.

Keys to hardening storage infrastructure

This combined approach ensures much higher levels of cyber security for enterprise storage, which is critical because today, reliance solely on backup is no longer enough. Primary storage has become a main target of cyber criminals for the most insidious and hard-to-detect ransomware and malware attacks that wreak costly havoc on enterprises. Combining cyber storage resilience (the ability to instil defensive security measures to repel attacks), detection (the ability to know when data is corrupted and whether a known good copy of data is free of ransomware or malware), and cyber recovery (the ability to recover known good data) from cyber attacks, are the keys to hardening enterprise storage infrastructure.

Triple play cyber security from Infinidat

Designed to deliver industry-leading application performance, InfiniBox®, InfiniBox™ SSA and InfiniGuard® are used extensively as backup targets for many data protection scenarios, backing up critical data assets across applications and virtual and containerised infrastructures. Whether it's for primary storage or secondary storage for backup and data protection, Infinidat has all the use cases covered with InfiniBox as a target and InfiniGuard as a purpose-built backup appliance. Here's why this approach is so important and how Infinidat's next-generation data protection solutions address these needs:

Proactive, risk based approach to cyber storage resiliency

With the increasing sophistication of cyber threats, enterprises need to build cyber storage resilience into their systems to withstand and adapt to attacks. The new legislation will require enterprises to take a risk-based approach and implement appropriate security measures, which aligns with the concept of cyber storage resiliency.

Infinidat's award-winning InfiniSafe® suite provides extensive cyber storage resilience capabilities, including InfiniSafe® Cyber Detection and InfiniSafe® Automated Cyber Protection (ACP) along with the stack of all the core pillars of next-generation data protection. InfiniSafe provides secure, end-to-end capabilities to orchestrate with existing security solutions to detect, contain, mitigate, and recover from a cyberattack.

InfiniSafe ACP is an early-warning system that seamlessly integrates into an enterprise's existing cyber security applications and systems. ACP triggers creating immutable snapshots when an event or threat is detected by your data centre-wide cyber security software or your Security Operations Centre (SOC).

Detecting a threat before it has an opportunity to propagate is critical to reducing the threat window. The solution integrates with existing cyber security infrastructure like an enterprise's SOC, or the enterprise's cyber security SIEM and SOAR software, which aligns with the Cyber Security and Resilience Bill's focus on ensuring that proactive cyber security measures are in place.

Automated threat detection

Rapid identification of threats is crucial to minimise the impact of a cyber attack. In common with NIS2 and the United States' Security and Exchange Commission's cyber security public reporting laws, the new Cyber Security and Resilience Bill will require more stringent incident reporting requirements, including reporting significant incidents within 24 hours.

Infinidat's solution to this is InfiniSafe Cyber Detection, which uses comprehensive machine learning to detect ransomware and malware, using 200+ content analytics points with up to 99.99% accuracy. This deep scanning capability helps identify compromised data quickly and precisely, enabling rapid identification of compromised data, in line with new legal requirements.

Instantaneous data recovery

Quick and effective recovery is essential to minimise downtime and data loss after an attack. Given the levels of disruption to critical services during the aftermath of recent attacks, the new cyber security legislation will emphasise the importance of ensuring business continuity with water-tight disaster recovery plans.

The InfiniSafe solution provides virtually instantaneous data recovery, with a guaranteed recovery time of 1 minute or less for Infinidat's InfiniBox family and 20 minutes or less for Infinidat's InfiniGuard purpose-built backup appliance. This rapid recovery capability aligns perfectly with the legal requirement within the Cyber Security and Resilience Bill, to ensure continuity of essential services.

In addition to facilitating cyber detection, robust protection, and the fastest possible recovery times, Infinidat's solutions can also help enterprises to be as proactive as possible in mitigating the risk of penalties. By addressing cyber storage resilience, detection, and recovery, enterprises can create a multi-layered defence against the ever-evolving cyber threat environments.

The triple play approach focuses on "shrinking the threat window" by automating protective measures at the speed of compute, reducing the time attackers have available to proliferate data corruption or encryption. Providing the ability to integrate with existing security infrastructure ensures that the storage layer becomes an active part of an enterprise's overall cyber security strategy.

By implementing solutions like Infinidat's InfiniSafe software suite, enterprises can create a more robust and effective cyber security strategy that addresses the full lifecycle of cyber threats - from prevention and detection to rapid recovery. This holistic approach is essential in today's landscape of sophisticated and evolving cyber threats, where traditional, siloed security measures are no longer sufficient.

We are in a leadership position to help enterprises better understand how to incorporate a cyber-centric, recovery-focused strategy, by integrating InfiniSafe capabilities into their overall enterprise cyber security strategy.

There is plenty of evidence that cyber attacks have evolved to increasingly target enterprise storage infrastructure and, in a data-driven economy, this cannot be allowed to happen. Infinidat's approach, to combine cyber storage resilience and cyber security to secure enterprise storage, closes the gap and vastly improves the ability to mitigate the impact of cyber attacks, especially ransomware.

We will continue to strive for broader awareness among CIOs, CTOs, and CISOs of best practices in cyber storage resilience and cyber recovery to help enterprises detect, restore, and recover from what are now inevitable cyber attacks.

Strategic IT planning must take cyber resilient storage into serious consideration, and Infinidat is a leading vendor on the cutting edge of this crucial advancement in securing enterprises against cyber attacks.

DW ROUNDTABLE

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

- Based around a hot topic for your company, this 60-minute recorded, moderated zoom roundtable would be a platform for debate and discussion
- Moderated by an editor, Phil Alsop, this can include 3 speakers
- Questions prepared and shared in advance
- There would be an opportunity to view and edit out any unflattering bloopers

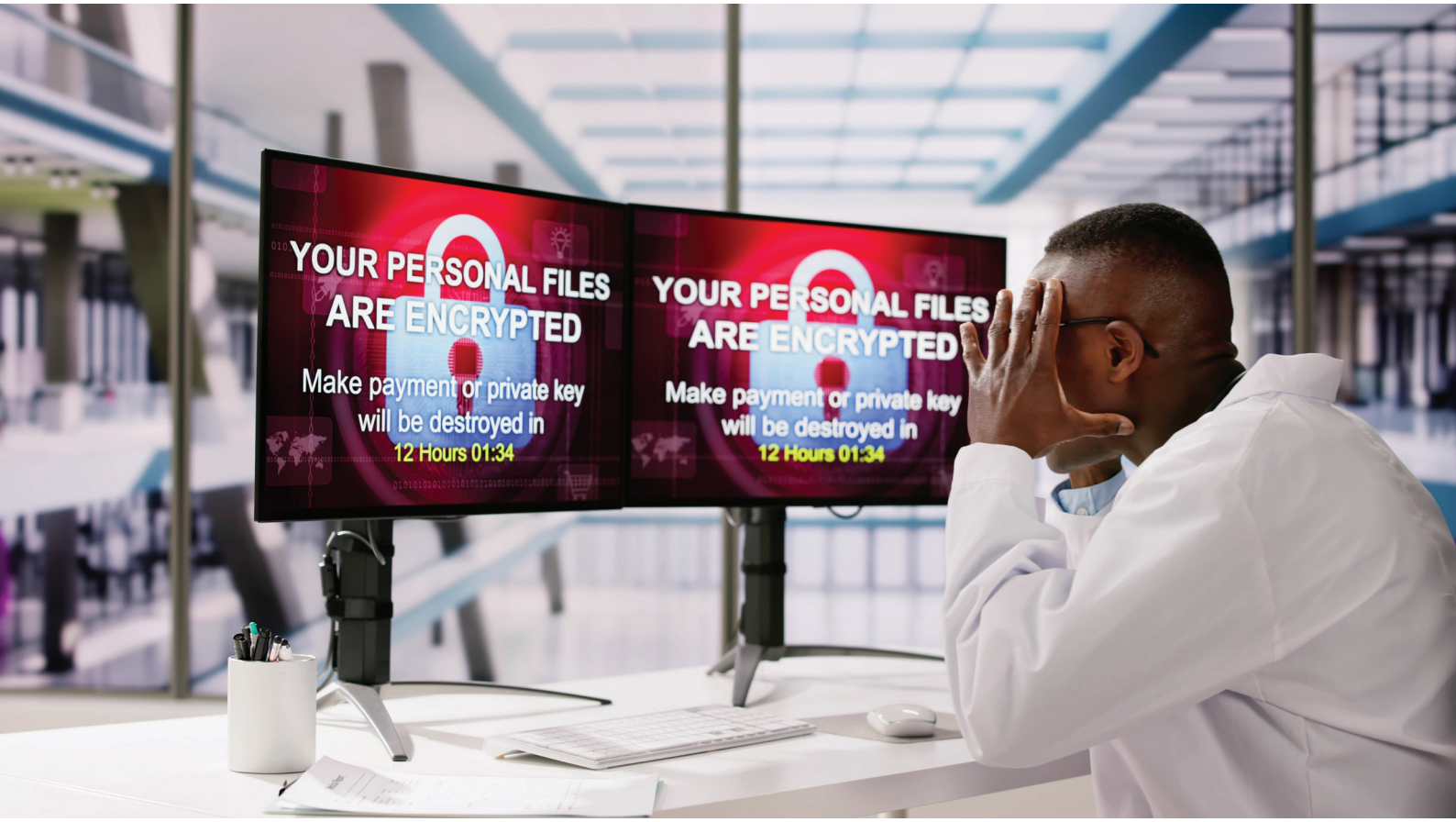
This event would be publicised for 4 weeks through all our mediums including:

- A banner on the Compound Semiconductor homepage for 8 weeks
- 4x weekly dedicated HTMLs
- 4x news pieces which would also appear on the weekly e-newsletters
- Promoted through our social media platforms for 8 weeks (pre and post event)
- Available as an on-demand asset through all mediums
- All registered attendees' details would be made available to you

Cost: €5995

Contact: Jackie Cannon at jackie.cannon@angelbc.com

ANGEL EVENTS



Strategies for making low-code applications cyber resilient

In 2023, one in four application breaches consisted of stolen credentials and vulnerabilities. Furthermore, 75% of all applications have at least one flaw. This is an alarming reality regarding application security – but it doesn't need to be this way.

BY FRANK BAALBERGEN, CHIEF INFORMATION SECURITY OFFICER, MENDIX

IN THE DIGITAL-FIRST WORLD, technology leaders have increasingly turned to low-code applications to accomplish business goals quicker than traditional development. However, some IT professionals have expressed concerns about security and data management specifically for low-code platforms. A third of these professionals reference the lack of low-code governance as the most serious security risk. Meanwhile, 26% of participants did not trust the app development platform.

Despite these concerns, Gartner estimates that the adoption of low-code/no-code technologies will increase from almost 25% of applications in 2020 to 70% in 2025, indicating that their ascent and popularity are not slowing. It is because low-code has impacted numerous organisations' digital transformation efforts by making it easier to run and create apps.

However, the rise of citizen coders has raised unique concerns among CTOs and technology leaders. They are concerned about managing these personnel groups while allowing them to remain innovative. The 'why' behind the security risk stems from a shortage of skilled professionals and the imperative to upskill existing employees who will, by default, not be as knowledgeable about keeping systems safe and secure.

Limited cybersecurity expertise in this fast expanding sector exposes vulnerabilities,

underlining the importance of proactive training to strengthen companies' defences and reduce risk. Below, we look at three actions businesses can take to make low-code platforms more cyber-resilient:

Championing data security

Organisations should ensure data security in low-code platforms complies with regulations, protects sensitive information, and maintains trust. Low-code platforms facilitate rapid development but pose risks if security measures are overlooked. Breaches can result in legal penalties, reputation damage, and loss of customer confidence. Implementing robust security protocols, including encryption, access controls, and regular audits, is essential.

Vulnerabilities in third-party components should be addressed through patch management and security updates. Preventing insider threats is equally important, requiring strict access controls and monitoring mechanisms. By prioritising data security, organisations can safeguard intellectual property, maintain business continuity, and uphold their commitment to protecting customer data, thus fostering trust and mitigating potential risks.

Incorporating security by design

Technology leaders should also encourage a security-first approach, including security safeguards in the development process, especially for low-code platforms. To protect their low-code platforms from cyber attacks, developers should use built-in security features. One important approach is to default to the least amount of resource access possible, reducing the chance of design flaws that result in incorrect data rights. This method is consistent with platform-based solutions, where allowing access is expressly needed, lowering the risk of data privacy and integrity.

Another area organisations could look to implement is a system that provides fail-safe defaults inside entity access methods, such as restricting default permissions to new entity characteristics. This guarantees that developers explicitly grant users access rights to newly introduced data characteristics, improving overall data protection measures. Low-code platforms force developers to explicitly provide users access to newly introduced data characteristics by limiting default permissions to new entity attributes.

Furthermore, it is critical to address the possible risks of depending entirely on a single security method, which might result in a single point of failure. Instead, a layered approach to security, which includes various checkpoints such as the domain model, microflows, and pages, guarantees a strong defence.

Implementing security controls in these three critical areas before allowing production access may considerably decrease the risk of unauthorised data access or breach. This multi-layered approach improves security resilience and gives users and stakeholders confidence in the platform's capacity to protect sensitive data.

Enforcing security training and awareness

Organisations should educate developers, administrators, and end users on cybersecurity best practices and possible dangers, which is critical for building a strong security culture. Platforms that provide extensive training resources and community forums are critical for arming stakeholders with the information they need to minimise risks successfully.

These platforms enable users to make educated decisions and take proactive security steps by offering easy access to learning about security best practices and staying up to speed on emerging risks.

It is also imperative to have regular cybersecurity training and awareness sessions within low-code development sectors. This empowers developers with the knowledge to mitigate risks effectively, ensuring that security remains a top priority throughout the development lifecycle.

The rising popularity of low-code platforms creates both benefits and risks regarding cybersecurity. To protect these platforms from cyber attacks, businesses must promote data security, including security by design principles, and implement frequent cybersecurity training and awareness sessions.

Organisations can enhance the cyber resilience of their low-code platforms and confidently manage the expanding threat landscape by emphasising proactive measures and providing stakeholders and developers with the required information and tools.

How the synergy of no-code and AI helps enterprises maximise automation through citizen development

Current economic conditions are pushing businesses to rethink their conventional staffing approaches, particularly in IT departments. Here the talent shortage has become particularly acute, with the demand for skilled professionals far exceeding supply.

BY DARREN LEWIS, CSO EUROPE

THIS IMBALANCE is being exacerbated by financial pressures that compel businesses to do more with less, making the efficient allocation of IT resources a strategic need.

Simultaneously, the digital arena has emerged as a critical battleground for companies striving to attract, engage, and retain customers. This shift is underscored by the expectation for seamless, intelligent, and personalised digital interactions. The pressure is particularly intense on traditional sectors, such as manufacturing, professional services, banking, and healthcare, which are being challenged to significantly augment their digital presence. These industries must refine both their internal operations and customer engagements with smart, automated solutions that can meet the elevated expectations of today's digital-savvy consumers.

This dual pressure of optimising IT operations and enhancing customer interactions highlights the limitations of traditional software development approaches, which are often slow, rigid, and require specialised skills. As a result, there is a growing recognition of the need for a new breed of problem-solvers — citizen developers. These individuals can utilise AI-assisted no-code platforms to rapidly develop and deploy solutions that address specific business needs without the need for extensive programming knowledge and do this much faster than their tech-savvy counterparts. The importance

of time-to-market cannot be overstated here; the ability to quickly adapt and launch products is a crucial competitive advantage in today's fast-paced market.

This scenario sets the stage for a transformative approach in how technology is leveraged within enterprises. The advent of AI-assisted no-code development platforms is enabling businesses to democratise the creation of applications, thereby empowering non-technical staff to contribute directly to digital solutions. By doing so, organisations are not only addressing the immediate challenges posed by the economic environment and IT talent crunch but are also positioning themselves at the forefront of digital innovation and customer engagement.

The strategic shift to citizen development and ai-assisted development

As businesses navigate this new landscape, emerging technologies such as Generative AI (GenAI) and no-code platforms are revolutionising industries with their transformative potential. These innovations are not merely altering the technological landscape; they are fundamentally enhancing the way we live and work. The rapid growth in the popularity of these tools is a testament to their profound impact on companies' capabilities. By aiding in decision-making, catalysing change, influencing behaviours, and increasing employee satisfaction, they not only elevate leadership qualities but also automate repetitive tasks, significantly boosting productivity and opening new avenues for creativity and innovation.

Meanwhile, the concept of citizen developers is revolutionising how organisations approach software development. By enabling individuals without formal programming backgrounds to create applications, no-code platforms are democratising innovation. Traditional no-code platforms broaden accessibility to the application development process by providing no-code creators with drag-and-drop tools. GenAI can further enhance this process by converting user-provided requirements into application templates or frameworks. This strategic shift allows businesses to rapidly adapt to market changes, consumer behaviours, and internal needs with unprecedented agility without burdening IT resources.

Empowering teams with No-Code and Ai to automate operations

The significance of no-code creators is on the rise due to their expertise in rapidly building and launching applications that are finely tuned to the organisation's needs. With a deep understanding of internal workflows and obstacles, they design applications that not only fit specific business contexts but also have the potential to grow into robust, enterprise-level solutions, offering sophisticated functionality and scalability essential for the organisation's operations.

With no-code creators leading the way, automation becomes a pivotal force for transformation, offering businesses the opportunity to streamline processes, enhance efficiency, and reduce operational costs

With no-code creators leading the way, automation becomes a pivotal force for transformation, offering businesses the opportunity to streamline processes, enhance efficiency, and reduce operational costs. The integration of AI with no-code platforms is particularly transformative, enabling organisations to leverage the power of automation across a broader spectrum of their operations without the need for extensive coding knowledge.

This synergy allows for the rapid deployment of automated solutions that can adapt and evolve in real-time, meeting the dynamic needs of businesses and their customers. By democratising the ability to create and implement sophisticated automated systems, no-code and AI are not just responding to the current challenges; they are reshaping the future of how businesses operate, making automation accessible to a wider array of users within the organisation and fostering a culture of innovation and agility.

Building No-Code creator talent

To promote the growth of citizen developers, organisations must adopt strategic approaches to identify and support this burgeoning talent. With guiding resources like the No-Code Playbook, a vendor-agnostic 200-page guide that empowers teams to deliver business applications of any complexity with no-code, organisations can evaluate the difficulty of their projects and select strategies that yield maximum efficiency, while maintaining utmost security.

The establishment of a No-Code Centre of Excellence (CoE) is a vital step in promoting a no-code culture within an organisation. The CoE plays a pivotal role in the recruitment, training, certification, and development of no-code professionals. Additionally, it assists delivery teams in adhering to governance and policy standards, ensuring a controlled yet collaborative environment for no-code development.

The initial step includes recognising potential citizen developers within the workforce. These individuals are often employees who exhibit a strong interest in technology, possess problem-solving capabilities, and have an in-depth understanding of company processes. They might already be devising solutions informally or demonstrate a tendency toward innovative thinking.

Training is pivotal in fostering citizen developers. Although this training need not be exhaustive or highly technical, it should equip employees with the necessary knowledge and confidence to begin. Mentorship is another critical component. Connecting aspiring citizen developers with seasoned mentors enhances the likelihood of a successful transition. These mentors can assist them in navigating the complexities of software development, ensuring that the solutions they create are robust, scalable, and secure. Establishing a supportive work environment is also crucial. This includes promoting experimentation and innovation, while providing a safety net for failure. An environment that values creative problem-solving and encourages employees to take calculated risks is vital for the flourishing of citizen developers.

By implementing these strategies, organisations not only tackle the immediate issue of developer shortages but also foster a culture of continuous innovation and adaptability. In the coming year, citizen developers are anticipated to play an increasingly significant role in software development and business growth.

These developers are set to significantly enhance organisational agility in responding to market shifts and customer needs. This evolution represents a natural progression, and organisations must quickly and effectively adapt and embrace it. The future of software development depends on it, and it's a change that the industry must embrace.

Building a Future-Ready workforce

The empowerment of citizen developers through no-code platforms augmented with AI is more than a strategic initiative; it's a commitment to building a future-ready workforce. As employees become more adept at leveraging these technologies, they not only contribute to the organisation's digital transformation efforts but also develop valuable skills that are increasingly important in the digital economy. The journey toward embracing citizen development, powered by no-code platforms and enhanced with AI, is a transformative one. This approach not only addresses the immediate challenges of the software development skills gap and the pressures on IT departments but also fosters a culture of innovation and agility that will sustain businesses in the long term.

Organisations that recognize the potential of no-code and AI, and invest in empowering their employees as citizen developers, will not only navigate the challenges of today's digital landscape more effectively and retain a competitive advantage, but will also shape the future of innovation. The power of no-code infused with AI capabilities lies not just in the technology itself but in the people it empowers, the problems it solves, and the futures it enables.

APC™

40Years

Make greater

IMPACT

with an industry-leading network

Celebrate 40 years with APC.

Start leveraging four decades of uninterrupted protection, connectivity, and unparalleled reliability with the APC UPS family, a legacy marked by pioneering UPS technology and an unwavering commitment to innovation.

https://www.apc.com/uk/en/product-category/88972-uninterruptible-power-supply-ups/

Life Is On Schneider Electric

Low-code platforms reshaping enterprise development

Low-code platforms have become mainstream and are here to stay. These platforms are revolutionizing software development, empowering organisations to build applications rapidly and efficiently.

BY VARUN GOSWAMI, HEAD OF PRODUCT MANAGEMENT, NEWGEN SOFTWARE

FROM SELF-SERVICE portals to business process automation, low-code is solving a myriad of enterprise-wide needs across various industries. The future holds even more possibilities, including advanced use cases in technologies such as RPA, AI/ML, and chatbots. In this blog, we'll delve deeper into the transformative impact of low-code platforms and explore their role in reshaping enterprise development.

The digital revolution has fundamentally altered the way we approach software development. Traditional coding practices, once the exclusive domain of skilled programmers have given way to a new era of accessibility and efficiency through low-code platforms. These platforms have democratized the development process, enabling individuals from diverse backgrounds to create powerful applications without extensive coding knowledge.

Evolution of Low-code platforms

In recent years, low-code platforms have evolved significantly, simplifying application development with intuitive drag-and-drop interfaces and pre-built components. Gone are the days of laborious coding; building sophisticated applications has become extremely simple. From chatbots to enterprise-grade solutions, these platforms empower users to bring their ideas to life with ease.

The impact of Gen AI on Low-code platforms:

The integration of generative artificial intelligence (Gen AI) marks a significant milestone in the evolution of low-code platforms. Gen AI enhances the intelligence and adaptability of these platforms, enabling them to automate routine tasks. By harnessing the power of AI, developers can accelerate the development process and focus on high-level logic and creativity. The potential economic impact of Gen AI is immense, with estimates suggesting trillions of dollars in added value to the global economy by 2040.

AI Co-pilots and Code generators

In addition to Gen AI, AI-powered assistants such as co-pilots and code generators are further streamlining the coding process. These assistants leverage large language models (LLMs) to provide real-time assistance, suggesting code snippets, identifying potential bugs, and even generating unit tests. By augmenting human capabilities with AI,

developers can enhance productivity and produce higher-quality code in less time.

The future of Low-code platforms

Gartner predicts that low-code platforms will account for 65% of the IT and software development market before 2024. As low-code platforms continue to gain traction, questions arise about the future of traditional coding practices. However, it's important to note that these platforms are not rendering coding obsolete; rather, they are democratizing access to software development. While AI technologies such as Gen AI and AI co-pilots excel at certain tasks, low-code platforms offer a holistic solution that caters to a wide range of development needs.

Exploring the landscape of Low-code platforms

Low-code platforms have transformed the way businesses approach application development. With their user-friendly interfaces and intuitive features, these platforms have opened the doors to innovation for individuals and organizations alike. Whether creating self-service portals, automating business processes, or modernizing legacy systems, low-code platforms offer a versatile solution to a wide range of development needs.

The rise of Low-code in various industries

The adoption of low-code platforms extends across diverse industries, each with its own unique set of challenges and opportunities. In the healthcare sector, for instance, these platforms are used to develop patient portals and streamline administrative processes. Similarly, in the finance industry, low-code platforms facilitate the creation of fintech applications and automate compliance procedures.

From manufacturing to retail, low-code platforms are revolutionizing how businesses approach software development, driving efficiency and innovation across the board.

The role of Low-code in modernisation efforts

Legacy systems pose a significant challenge for many organizations, hindering agility and innovation. However, low-code platforms offer a pathway to modernisation, allowing businesses to update and enhance their existing systems without the need for extensive redevelopment. By leveraging low-code platforms, organizations can breathe new life into legacy applications, improving functionality and user experience while reducing costs and development time.

According to Microsoft's Low-Code Signals 2023 report, 87% of Chief Innovation Officers and IT experts believe that integrating increased AI and automation into low-code platforms would significantly enhance their ability to leverage the range of capabilities available fully. Low-code platforms facilitate broader development horizons when paired with GenAI, which enhances efficiency and alignment. It applies machine learning algorithms to streamline the development processes.

Low-code combined with GenAI holds the potential to simplify and automate business processes. Thus, democratizing the development process expands possibilities and enables a more comprehensive array of individuals to engage in the creation of technological solutions.

The Importance of accessibility and inclusivity

One of the most significant advantages of low-code platforms is their accessibility. By lowering the barrier to entry for software development, these platforms empower individuals from diverse backgrounds to participate in the digital economy. Whether a small business owner is looking to create a mobile app or a non-profit organization is seeking to streamline its operations, low-code platforms offer a level playing field for innovation and growth.

Furthermore, low-code platforms foster a culture of collaboration and creativity by embracing inclusivity and diversity, driving positive change and societal impact.

Conclusion

The rise of low-code platforms represents a paradigm shift in software development. By democratizing access to application development and embracing emerging technologies, these platforms are reshaping how we approach software development.

As we continue to explore the possibilities of low-code, we unlock new avenues for innovation and growth, driving positive change and transformation across industries. With the power of low-code at our fingertips, the future of software development is indeed bright and full of potential.

One of the most significant advantages of low-code platforms is their accessibility. By lowering the barrier to entry for software development, these platforms empower individuals from diverse backgrounds to participate in the digital economy

Drilling down on cloud-native software

On the surface, breaking up monolithic applications into dozens or hundreds of independent cloud services can seem more complicated. In practice though, cloud-native principles make software easier to write, deploy, and maintain.

BY KIRAN BHAGESHPUR, CTO AT QUMULO

WAY BACK at the dawn of the Computer Age, on a flight to Albuquerque to visit potential investors, Paul Allen realized he had a problem. He was on his way to show MITS executives the BASIC interpreter that he and Bill Gates had written for the Altair 8080 one of the first microcomputers. But they'd forgotten to include a routine to actually read the program (written entirely on paper tape, an early form of storage) into system memory. Allen, never one to shrink from a challenge, dashed off a bootstrap loader midflight. And the rest is history.

Of the many lessons to take from this tale, one of the biggest is just how much software has changed over the last several decades. Allen's problem was that, in those early days, software was fully "aggregated." To write a computer program, you had to code out everything – not just how the application itself would behave, but detailed instructions for assembling all the resources needed to run it.

Since then, computing has undergone a steady process of disaggregation, splitting off various components (like processor resources, networking, and storage), so they can operate independently as common cloud services. Developers can then simply connect those existing services to their applications instead of continually recreating from scratch.

Fast forward to today, and we're taking disaggregation to the next level, breaking up monolithic applications into even more granular microservices, each handling a specific function, each optimized to run in the cloud. This is the essence of "cloud-native" software, even if it's not always described in those terms. But if you're evaluating a cloud-native software investment, and you want to understand what it will mean for your business, disaggregation is a great place to start.

Disaggregating the cloud

From the get-go, cloud and disaggregation have been inextricably linked. Indeed, it's the ability to treat computing infrastructure as independent common services that makes cloud so valuable. Consider a retail business using an eCommerce application. In the past, they would have had to build and maintain the full hardware infrastructure to run that software. Usually, that would mean overprovisioning to ensure they could handle peak traffic loads – even if most of the time, that infrastructure investment would be massively underutilized.

Today, retailers can run their applications in the cloud and consume computing, network, storage, and other resources on demand. Instead of investing for peak capacity, they can use exactly the cloud resources they need as they need them, scaling services out and in with demand, and paying for only what they use. It's why cloud has been among the fastest-growing innovations in the history of computing.

Going cloud-native

Now, we're entering the next phase of disaggregation with "cloud-native" software, or software written specifically for cloud environments, designed to take full advantage of cloud capabilities. In many ways, this shift is just the latest chapter in the ongoing disaggregation story, but it introduces big changes to

how software is written and deployed. To be truly cloud-native, software must be:

- **Microservices-based:** More than just splitting off infrastructure resources, cloud-native applications break down software into even more granular "microservices," each running in standardized containers on a common architecture. As a result, each individual application function can now benefit from on-demand scalability and resiliency, using consistent and predictable cloud services.

- **Portable:** Because microservices run in standardized containers, cloud-native software can be moved from one platform to another much more easily.

- **Designed to interact with cloud primitives:** Cloud-native applications don't have to include explicit instructions for managing the IT resources they need. Instead, they're written to call on existing cloud services (for example, Amazon's AWS-native S3 storage service). In addition to making software easier to write and deploy, this change has sparked a rapidly growing ecosystem of third-party cloud services. As more developers write cloud-native software, more third parties are incentivized to create new services their applications can use, feeding a virtuous circle.

- **Manageable as code:** When software is designed to run in cloud environments, drawing on common cloud resources that work in consistent ways, deployments become much easier. It's now possible to spin up a new application with a few lines of code and start using it in minutes—avoiding the weekslong installation and configuration process of traditional on-prem software.

The cloud-native advantage

On the surface, breaking up monolithic applications into dozens or hundreds of independent cloud services can seem more complicated. In practice though, cloud-native principles make software easier to write, deploy, and maintain. Among its many advantages, cloud-native software provides:

- **Elasticity:** Now, you can scale all application components and resources – not just infrastructure – in and out with demand, and readily accommodate unexpected spikes in utilization. You can also respond to evolving resource requirements more easily. Many years into the making Avatar: The Way of Water, for example, James Cameron found that the cutting-edge special effects he wanted would require as much as 1.6 billion hours of virtual CPU cycles to render. The job was far too big for his effects company's data center, and upgrading would have taken too long and carried exorbitant costs. But providing resources at that scale was no issue for the cloud.

- **Improved resiliency:** Along the same lines, when software is designed from the ground up to take advantage of common cloud availability and resiliency services, you can absorb and recover from problems much more effectively.

- **Increased productivity:** With cloud-native software, common processes (load-balancing, scaling, recovery) are handled automatically by cloud orchestration tools like Kubernetes – which means developers don't have to code out explicit instructions for managing them. Instead, they can call on a large, growing number of pre-existing cloud services. In fact, cloud-native software typically requires a fraction of the coding of traditional applications, and can often can be written in weeks instead of months or years.

- **Improved business agility:** With cloud frameworks and services automating many aspects of development and deployment, businesses gain more flexibility and speed. It becomes much easier to continually update cloud-native software and continually bring new capabilities to users. For the same reason, you can now try out new software innovations more quickly, with far less risk.

Individually, each of these cloud-native software benefits would be extremely valuable. Together, they're nothing short of revolutionary. We can thank the ongoing disaggregation of computer applications for making them possible.

On the surface, breaking up monolithic applications into dozens or hundreds of independent cloud services can seem more complicated. In practice though, cloud-native principles make software easier to write, deploy, and maintain

Shift Left:

How Database DevOps creates stronger and more streamlined database operations

When things go wrong, people are often quick to point the finger of blame. And when it comes to information technology and especially application performance, the database is one of the first components to be singled out.

BY KEVIN KLINE, SOLARWINDS DATABASE TECHNOLOGY EVANGELIST

INDEED, some database practitioners and experts estimate up to 70% of all application performance issues can be blamed on databases.

The issues affecting databases are typically either the poor quality of SQL code, bad administrative practices, or poor governance. So, what may have once been regarded as an asset can quickly become a costly and time-consuming burden, especially on teams without a talented database professional or DBA.

Instead of delivering the benefits associated with a data-driven organisation, such shortcomings can cause operational inefficiencies exposing businesses to unnecessary risk and poor performance.

And yet, there is a solution. By incorporating database application development into DevOps, those responsible for the integrity of databases and related systems can help ensure data and applications run efficiently.

DevOps can bolster databases

DevOps is a set of practices aimed at enhancing collaboration and communication between development (Dev) and operations (Ops) teams. It is aligned to automation, continuous integration, and continuous delivery (CI/CD) to help IT professionals achieve better results via a culture of efficiency, collaboration, and rapid, iterative delivery.

Should the worst happen, DevOps helps businesses and other organisations avoid downtime, reduce deployment rollbacks, tighten security, and eliminate system crashes. That's because application development teams who use CI/CD can quickly rollback software updates, including changes to the database, with ease.

But there is a problem. The increasingly complicated nature of the data upon which so many organisations rely means companies often struggle to bring data into their DevOps framework. As a result, many businesses steer clear, preferring not to get tied up by a tangle of database complexity.

By improving database visibility, they can integrate data, database schemas, and stored procedure code into their DevOps practices in the same way that developer teams do with their application source code

As a result, teams canstreamline database development and design through a process known as Continuous Integration/ Continuous Deployment (CI/CD). Using the CI/CD process

can also enhancie security and reduce the possibility of downtime and system crashes. In fact, there is a branch of DevOps which seeks to emphasize security earlier in the development process called DecSecOps.

In a similar way, smart dev teams could introduce database observability solutions to reveal the inner workings of their database systems, thus delivering "DevPerfOps". Crucially, bringing performance observability early into the development process enables IT professionals to see inside the black box, understand the root cause of performance issues, resolve issues faster, and proactively optimise poor performance to help prevent future issues. Compare the forward-looking perspective of DevPerfOps to the typical approach of dev teams, i.e. roll out a new application without evaluating performance, then attempt to improve performance based upon user complaints. Seems backwards, doesn't it?

Even better, incorporating observability into the DevOps framework becomes much easier once your databases themselves are under observation. There is an industry term used to describe moving an element from late in the development process. It's known as "Shift-left". By shifting left with security, developers ensure that security is not an afterthought (and a gaping security hole) in their applications. In the same way, shifting left with application performance means that developers do not have to plan to constant performance tweeks once their application has moved to production.

If you're still in any doubt about the benefits, here are six of the top benefits organisations can realise through this framework:

1. Streamlined deployment and software delivery:
Organisations can integrate database development and operations into DevOps to enable a streamlined and automated approach to software delivery. As a result, teams should be able to meet the needs of their business or organisation through faster deployment cycles and the delivery of new features and updates.

2. Increased collaboration across teams:
By bringing together developers, operations teams, and database administrators, businesses are better able to encourage collaboration and communication across different departments. This can lead to better alignment of goals, improved understanding of requirements and more efficient problem-solving.

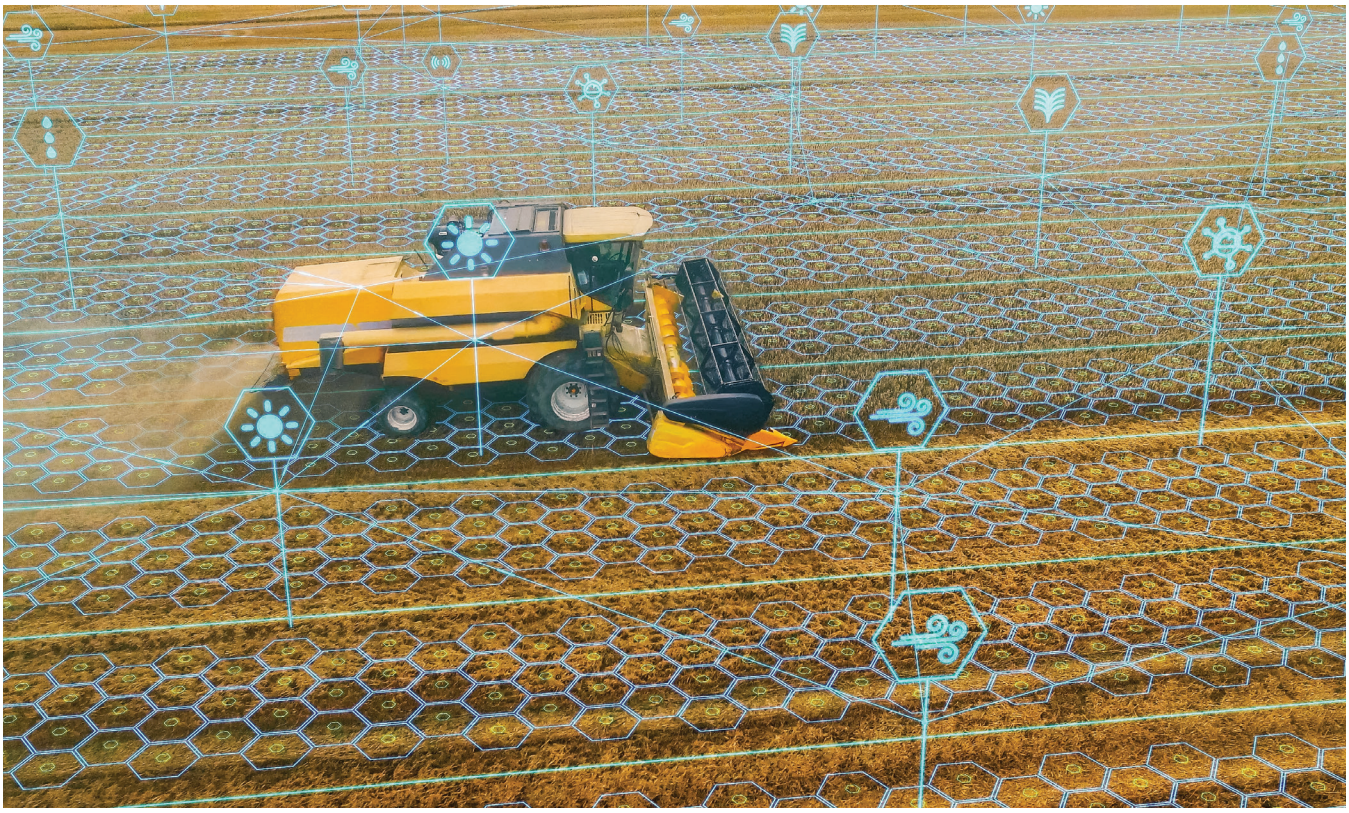
3. Improved agility and flexibility:
Organisations need to respond rapidly to evolving business needs and market demands — no matter where they are on their digital transformation journeys. By automating database provisioning, configuration, and deployment as they do with their application code, teams can more easily scale their infrastructure, roll out new features, and adapt to the evolving needs of the business.

4. Reduced risk and downtime:
By automating and standardising database deployments using CI/CD, organisations can minimise the risk of human errors and reduce the potential for downtime. Database DevOps practices can help ensure changes are thoroughly tested and validated before being deployed. This reduces the chances of data loss or service disruptions. And if deployment of new database code goes wrong, CI/CD can make it quicker and easier to roll back to the last good version.

5. Efficient database management:
Virtually all applications within an organisation require a database. Implementing DevOps that includes the database code and design gives organisations a structured approach to managing databases and any data changes through version control. This approach to tracking and managing changes to software code guards against any 'uncontrolled' changes, structure, or configuration of a database. This means it's easier to rollback a faulty software release, helping to ensure changes can be managed efficiently and safely, or even reversed when needed.

6. Improved compliance and security:
Database DevOps emphasises including security and compliance measures throughout the development lifecycle. By integrating security controls and best practices, organisations can factor in data protection, privacy, and regulatory compliance requirements earlier in the process.

By integrating your databases into your DevOps process, the disparate teams within an organization (IT operations, DevOps teams, and database administrators) can help ensure that their database infrastructure realises the same benefits as other application development teams using DevOps. Not only can organisations implementing database observability and a DevOps framework that caters to the complex needs of their diverse and growing business requirements, but it can also help them design robust database architectures, fulfil database performance needs and drive successful digital transformation and modernisation initiatives.



Code optimisation:

The key to a more sustainable future for AI

Google's recent disclosure of a 48% increase in emissions over the past five years, largely due to the energy demands of its data centres, has highlighted the environmental impact of artificial intelligence. While this issue was previously underreported, the substantial computing power and energy consumption required by the rapidly advancing AI industry are now coming into focus.

BY DR LESLIE KANTHAN, CEO OF TURINTECH

AS COMPANIES increasingly integrate AI into their products, processes, and services, the significant environmental consequences can no longer be overlooked. It's important to note that it's not only the training of AI models that adds to the carbon footprint; the continuous inference required to process requests and generate responses is also a major contributor.

To mitigate AI's environmental impact, comprehensive strategies are needed, including the use of green energy and advancements in hardware. However, one crucial yet often neglected factor is the efficiency of AI code.

While leadership teams, particularly ESG teams, are deeply concerned with reducing the institution's overall energy footprint, developers are focused on delivering functional code on time.

In this situation, simply encouraging developers to be mindful of energy use isn't enough; what's really needed is a process that can help reduce cloud bills while also enhancing the capabilities of developers.

By prioritising code optimisation, companies can achieve immediate reductions in the carbon footprint of their AI systems. This involves refining code to enhance performance and decrease energy usage, offering environmental and financial advantages.

What is code optimisation?

Code optimisation is the process of improving the efficiency of code so that it runs faster, uses less memory, or consumes fewer computational

As innovation becomes a necessity and organisations race to integrate transformative technology into their services, the reliance on and emissions from data centres will continue to rise. Our planet cannot afford to let data centres operate inefficiently

resources. However, it isn't just about making your software run faster; it's also a key lever for sustainability, especially in the age of AI.

We recently worked on a QuantLib project, where we uploaded an optimised version of their code and saw a remarkable 30% improvement in execution speed.

But how does this affect the environment? Take cloud computing as an example. If a company spends £100,000 annually on cloud resources, optimised code could reduce that cost to £80,000. Not only does this mean significant savings, but it also translates to lower energy consumption and reduced carbon footprints.

However, most developers, even the best ones, often write code with tight deadlines in mind, not with efficiency or sustainability as a priority. While a developer might refine their code if given unlimited time, they rarely consider aspects such as whether they're maximising CPU usage or allocating memory efficiently.

This lack of focus on optimisation is understandable, particularly when managing codebases that span millions of lines. It could take years for teams to manually refine such code.

So, how do we make optimised code attainable?

How can it work?

One way that this can be achieved is through automation. By leveraging the power of large language models (LLMs), businesses can now streamline code optimisation and generation processes. The key advantage is the significant reduction in time—companies not only achieve more efficient software but do so in just minutes, greatly alleviating the typical time constraints of these processes.

This approach optimises code to perform more tasks with fewer computational resources. As a result, tasks that traditionally require substantial energy now consume much less power. Since energy consumption is closely linked to software efficiency, adopting this method can lead to substantial energy savings. These energy savings translate into lower carbon emissions from data processing, storage, and software operation, directly reducing a company's scope one and scope two emissions. Code optimisation can also help lower scope three emissions, such as those associated with products sold.

Additionally, businesses can obtain specific CO2 reduction percentages and energy consumption metrics, which can be used to demonstrate a tangible commitment to sustainability – a crucial factor in light of upcoming regulatory requirements.

The bottom line

The AI industry must adopt comprehensive, all-encompassing strategies to ensure it advances sustainability, rather than undermining it with each new development. Automating code optimisation could be the key to delivering immediate, sustainable solutions for AI.

As innovation becomes a necessity and organisations race to integrate transformative technology into their services, the reliance on and emissions from data centres will continue to rise. Our planet cannot afford to let data centres operate inefficiently.

Code optimisation offers a solution to this challenge. When considering the additional benefits of reduced costs, improved reliability, and increased flexibility, it is evident that this is the right path forward.

Generative AI could democratise network operations

Network operations is an expert field, and there's a good reason for that. These specialists comb through a network's raw data and analyse the problems and issues that emerge from it. In doing so, they keep the network – and business – running smoothly. It's a crucial function within the modern network, yet one that is facing an ever-mounting degree of friction.

BY PAUL GRAY, CHIEF PRODUCT OFFICER, LIVEACTION

THE AVERAGE business network has grown hugely in recent years. This age of digital transformation has introduced well-worn legacy infrastructure to new technologies. The IoT and the cloud have all fundamentally changed the way networks operate.

They've done this in two principal ways. Firstly, they've fundamentally changed the architectural form of a network. As new technologies and assets have been introduced, the network expands outside the sight or traditional range of vision, sitting outside the perimeter - such as IoT and cloud - and leaving a series of blindspots that teams cannot see into. One report from Dimensional Research estimates that 81% of operations teams struggle with network blind spots. Those blindspots create effective new breach points for attackers, new, unexpected pathways for traffic to emanate from and - to boot - new types of traffic.

Perhaps unsurprisingly, businesses now report that these new technologies and types of traffic are exactly the places they report visibility problems within. LiveActions 2024 Network Performance and

Monitoring Trends report (NPMT) showed 57% of organisations noted that they lacked visibility into relatively new areas like Cloud SD-WAN, Voice and Video.

Secondly, these transformations exponentially increased the load of traffic on a network. Some estimate that the average organisation's traffic volume has doubled, if not tripled, in the last five years.

The 2024 NPMT showed that respondents' current network performance management (NPM) solutions cannot keep up. Almost half of all respondents – 49 %—say that their current NPM can't provide insights that help them solve their current network problems. However, perhaps more importantly, 43% say that their NPMs cannot scale with the data volumes and network complexity they now deal with.

Tool sprawl

While the network management landscape has grown uncontrollably, the tools they use to manage it are often legacy solutions designed to view a type of network which we've long innovated in the past. On top of that, these tools usually accumulate quickly; according to one study, the average NetOps team uses up to 10 tools to monitor their network. According to another survey, almost a quarter of large enterprises rely on up to 25 network performance monitoring tools.

These are complex pieces of technology with their own user interfaces, programming languages, and metrics, and they often don't integrate. This creates a variety of data streams that look at different aspects of network operation but little understanding of the true nature of network behaviour. This kind of tool sprawl creates an inconsistent patchwork vision of the network, which ultimately increases confusion when it is meant to eliminate it.

Skills gaps

Dealing with this complexity is a series of over-stretched and understaffed network and security professionals. Much has been made of the global IT skills gap, with IDC predicting that by 2025, 90% of global organisations "will be staring down the barrel of a crippling IT skills gap."

The same is true in this case, where cybersecurity and network operations skills are in high demand while supply seems stubbornly lacking.

This results not just in skill deficits around critical network functions but ultimately stretches the time, focus, and energy of the experts present. Their effectiveness as experts must improve as they chase down false positives and manoeuvre between sprawled stacks of legacy tooling.

Generative AIs offer a way out

In short, many have arrived at an impasse. The load of increasing demands on network operations is now colliding with decreasing capacity. Yet, a new possibility exists in the explosion of generative AI technology that has ignited in the last few years.

The key here lies in its ability to take dense technical information and translate it into natural language. That's the key that could allow organisations to tame the uncontrollable growth of their networks and diminish their capacity to mitigate and monitor it.

This works in several ways. First, it mitigates complexity by offering natural language explanations of otherwise complex network issues.

If, for example, an NPM tool shows packet loss in a particular part of the network, a generative AI could deconstruct the event by offering an analogy, comparing it to a traffic jam that occurs at peak driving times and rush hour.

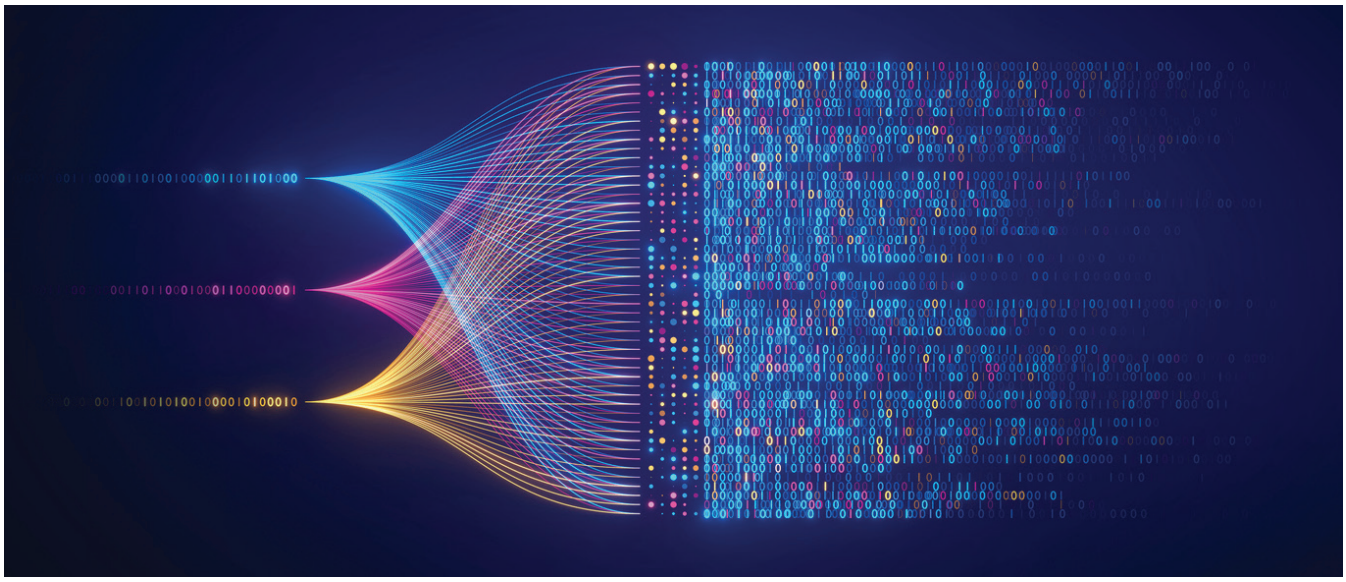
Secondly, one of the big problems that network engineers face is drawing a line between a tool's analysis and an actionable insight that might tell them what to do next. When an NPM tool shows that data transfers are slowing due to saturated bandwidth in the data centre, a generative AI can suggest implementing link aggregation by binding network links into a single connection, thus expanding the lane down which data transfers travel.

Finally, it fundamentally lowers the entry barrier for these otherwise specialised roles. Network operations staff are experts in their field, and that expertise can't be taken for granted. However, Generative AI provides a novel way to train new experts from existing staff and give precious time back to those network operations veterans whose attention and expertise are valuable.

Take the example of the protocol analyser - also known as a packet sniffer - which is one of the most essential tools in the network operations toolkit. When such a tool reveals, for example, a spike in TCP retransmissions, fledgling network engineers can use a generative AI to explain what that means and how to deal with it.

These technologies have come just in time for network operations specialists. They've spent the last few years seeing their workloads grow and their networks complex, putting out fires while they should have been using their expertise on strategic problems which might help a network innovate and enable business growth over the long term.

Generative AI can help collapse that mounting complexity and open the discipline of network operations to more people, thus expanding the talent pool a business can draw on to live up to this crucial function.



Five things you should know about AI networking

If your organisation has a data centre, it is likely AI technology will be deployed into it soon. Whether the AI system will be a chat bot, provide the automation of processes across multiple systems, or enable the analysis of large data sets, this new technology promises to accelerate and improve the way many companies do business. However, AI can be a confusing and misunderstood concept. In this article we'll explore five fundamental things you should know about how AI networking works and the unique challenges the technology faces.

BY LINAS DAUKSA, PRODUCT MANAGER, KEYSIGHT TECHNOLOGIES

A GPU is the brain of an AI computer

In simple terms, the brain of an AI computer is the graphics processing unit (GPU). Historically, you may have heard that a central processing unit (CPU) was the brain in a computer. The benefit of a GPU is that it is a CPU that is great at performing math calculations. When an AI computer or deep learning model is built, it needs to be "trained," which requires solving mathematical matrices with potentially billions of parameters. The fastest way to do this math is to have groups of GPUs working on the same workloads, and even then, it can take weeks or even months to train the AI model. After the AI model is built, it is moved to a front-end computer system and users can ask questions of the model, which is called inferencing.

An AI computer contains many GPUs

The best architecture to solve AI workloads is to use a group of GPUs in a rack, connected to a switch at the top of the rack. There can be additional racks of GPUs all connected in a networking hierarchy. As the complexity of the problems being solved increases, the greater is the need for GPUs with the potential for some implementations containing clusters of thousands of GPUs. Picture the common image of a data centre with rows and rows of computing racks.

An AI cluster is a mini network

When building an AI cluster, it is necessary to connect the GPUs so they can work together. These connections are made by creating miniature computer networks that allow the GPUs send and receive data from each other.

Figure 1 illustrates an AI Cluster where the circles at the very bottom represent workflows running on the GPUs. The GPUS connect to the top-of-rack (ToR) switches. The ToR switches also connect to network spine switches at the top of the diagram, demonstrating a clear network hierarchy required when many GPUs are involved.

The network is the bottleneck of AI deployments

Last fall, at the Open Compute Project (OCP) Global

Summit, where participants were working out the next generation of AI infrastructure, a key issue that came up was well articulated by Loi Nguyen from Marvell Technology: the "network is the new bottleneck"

GPUs are very effective at solving math problems or workloads. The fastest way for these systems to accomplish a task is to have the GPUs all collaborate on the same workload in parallel. To do this, the GPUs need the information that they will work on, and they need to communicate with one another. If a GPU does not have the information it needs, or it takes longer to write out the results, all the other GPUs must wait until the collaborated task is complete. In technical terms, the prolonged packet latency or packet loss contributed by a congested network could cause retransmission of packets and significantly increase the job completion time (JCT). The implication is that there can be millions or tens of millions of dollars of GPUs sitting idle, impacting bottom line results and potentially affecting time to market for companies seeking to take advantage of the opportunities coming from AI.

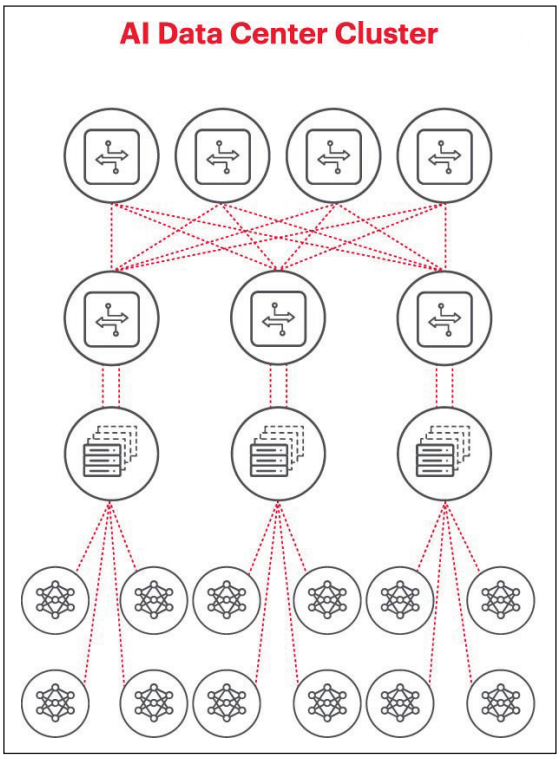
Testing is critical for successfully running an AI network

To run an efficient AI cluster you need to ensure that GPUs are fully utilised so you can finish training your learning model earlier and put it to use to maximise return on investment. This requires testing and benchmarking the performance of the AI cluster (Figure 2). However, this is not an easy task as there are many settings and interrelationships between the GPUs and the network fabric which should complement each other architecturally for the workloads.

This leads to many challenges in testing an AI network:

- The full production network is hard to reproduce in a lab due to cost, equipment availability, skilled network AI engineer time, space, power, and heat considerations.
- Testing on a production system reduces available processing capabilities of the production system.
- Issues can be difficult to reproduce as the types of workloads and the data sets can be widely different in size and scope.
- Insights into the collective communications that happens between the GPUs can be challenging as well.

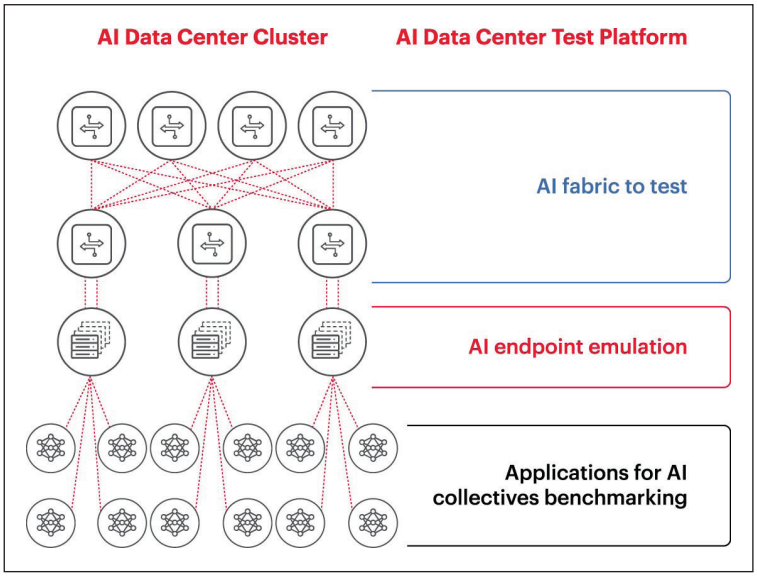
One approach to meeting these challenges is to start by testing a subset of the proposed setup in a lab environment to benchmark key parameters such as JCT, the bandwidth the AI collective can achieve, and how that compares to the fabric utilisation and buffer consumption. This benchmarking helps find the balance between GPU / workload placement and network design/settings. When the computing architect and network engineer are reasonably pleased with the results, they can apply the settings to production and measure the new results.



➤ Figure 1. An AI Cluster

Conclusion

In order to take advantage of AI, the devices and infrastructure of the AI network need to be optimised. Corporate research labs and academic settings are working on analysing all aspects of building and running effective AI networks to solve the challenges of working on large networks, especially as best-practices are continuously evolving. It's only through this reiterative, collaborative approach that the industry can achieve the repeatable testing and agility in experimenting "what-if" scenarios that is foundational to optimising the networks that AI is built upon.



➤ Figure 2. An AI data centre testing platform and how it tests an AI data centre cluster.

When network performance slows cloud applications and Gen-AI, think WAN acceleration

Generative artificial intelligence (Gen-AI) is the latest technology craze, but David Linthicum, Author of 'An Insider's Guide to Cloud Computing', and a contributor at InfoWorld, opines that most cloud-based generative AI performance stinks. What's lacking is basic computer architecture best practices, making these systems quite sluggish. This issue can arise with any cloud-based application because of the effects of latency, packet loss and poor bandwidth utilisation.

BY GRAHAM JARVIS – FREELANCE BUSINESS AND TECHNOLOGY JOURNALIST

AS FOR GENERATIVE AI's sluggishness, he comments: "Performance is often an afterthought with generative AI development and deployment. Most deploying generative AI systems on the cloud -and even without the cloud - have yet to learn what the performance of their generative AI systems should be, take no steps to determine performance and end up complaining about the performance after deployment. Or, more often, the users complain, and then generative AI designers and developers complain to me."

Phil Hill – a systems architect at Bridgeworks – explains that there was an incident in July 2023 with Photoshop's generative AI that led users tweaking their routes or connectivity to get around sluggish performance. There may be many reasons for this occurrence, which could include Wide Area Network (WAN) congestion on specific WAN links. Sometimes SD-WAN can avoid the congestion on certain links, allowing to reconfigure and even out the workload. He adds: "Forgetting AI for the moment, let's remember why software is written. Basically, need

is the mother of invention. What we are seeing is a plethora of new apps and solutions on a monthly basis addressing some sort of perceived need. However, the author of such systems only has specific tools in his toolbox – the ones he owns or understands."

Creating trade-offs

This means, that while there are many ways of doing things, a comparison with two vastly different methods will lead to trade-offs between them. Like with any network, the more people sharing, the slower the network can become because bandwidth becomes apportioned to each connected user. Then again, the spectres of latency and packet loss may also be playing a role – as expressed by Linthicum. Hill finds that the systems moving the most data will suffer the most, and it will be especially evident when they are geographically separated over large distances from each other.

"You also have to remember though that the AI itself is doing a few things to process the request – broadly it needs to understand the request, synthesise plausible responses, assess accuracy and ethical implications and respond," he explains.

Processing sluggishness

Consider, as well, that when the hardware processing is shared, there is bound to be some processing latency as there will be lots of service requests. This is a fact of processing data and hardware performance. "It's only when we transfer data that we can improve the outcome by using WAN Acceleration," he advises.

Performance is, nevertheless, seen as an afterthought in many cases – including with generative AI development and deployment. So, at this juncture, he notes Abraham Maslow's comment: "If the only tool you have is a hammer, you tend to see every problem as a nail." With regard to cloud applications more broadly, when the app relies heavily on database usage or distance related to data transfers, then similar issues of sluggishness can occur.

Determining performance

So, how should organisations determine what the performance should be of their cloud-based applications – including Gen-AI? His advice is to go back to basics because organisations should be aiming to establish some key performance indicators (KPIs). This requires them to research how people are currently completing a task, and how they can improve on their efficiency by doing something differently. They should also consider how long the task takes to complete, and how easy or painful the experience is. By analysing what works well and what doesn't, performance improvements can be attained.

With regard to performance, Hill says technologies such as SD-WANs and WAN Optimisation can resolve some cloud performance issues for Gen-AI and for cloud-based applications. This could be to the extent that the transfer of dispersed data can be sped up using these, but not database queries and generative processes.

Better results

However, they can't achieve the same results as WAN Acceleration. Hill explains: "Where data transfer has been identified as the bottleneck, and where the bandwidth is only minimally used, 90% bandwidth utilisation, using our PORTrockIT WAN and data acceleration appliances, but each case will be different." He recommends that organisations should assess the WAN needs of their cloud-based applications – including GEN-AI. This requires an investigation in how much data an organisation needs to transfer in order to specify their WAN bandwidth requirements. To start with, this is about analysing how many megabytes per second they need to transfer to do this.

He then advises that there should be a need to request bandwidths in excess of the current usage requirements. As part of the performance improvement, they should also consider WAN Acceleration technology to mitigate latencies of 5ms or higher.

Why the automated edge is the new frontier for business networks

The constant rush to adopt new technologies can quickly have an adverse effect on business networks – hindering bandwidth, connectivity, and eventually their bottom line. To overcome this problem, forward-thinking companies are now embracing the network edge. But what exactly is the edge? And how can it improve your operations without compromising latency, performance, or security?

BY PAUL GAMPE, CHIEF TECHNOLOGY OFFICER, CONSOLE CONNECT

IN GENERAL TERMS, the edge of a network is the boundary between your business network and the public internet. It's the zone where traffic from the internet enters your private network and vice versa. This zone is of critical importance because it defines your network security boundary and is the first line of defence against threats from the public internet. This includes firewalls, routers, switches, sensors, and other access points that exist at the boundary of networks.

Your network edge exists wherever there is an edge device or 'thing' that facilitates traffic crossing from one network to another. These edge devices can include mobile phones, laptops, data centres, company offices, home routers, and all manner of emerging applications that will become more commonplace as more users make up the rise of 'the internet of things'.

Of course, the sheer volume of data produced by these multiple devices can seriously hinder a company's network infrastructure, which can only process so much data without problems arising with bandwidth and lag time.

That's where edge networking comes in. This is a data management system that supplies digital resources to your users by merging edge devices with your business network to process and interpret data close to the source without the need for huge data centres.

Consequently, moving to the edge has become a key investment for businesses looking to deploy innovative technologies such as generative AI because they can now process data where it happens – at the boundary of edge devices – as opposed to in the cloud where latency and security issues abound. This not only helps to accelerate business decisions but also gathers valuable information at the point of origin to improve both product offerings and customer experiences.

What's more, businesses can vastly reduce data transfers over external networks, minimising the threat of data breaches while maximising bandwidth usage, and ultimately improving customer outcomes.

Benefits and drawbacks

A well-configured edge network can significantly improve the performance of applications that are hosted in the cloud. By placing edge devices closer to the users of these cloud-based applications, the distance that data must travel is greatly reduced, which means lower latency.

By placing security controls closer to this cloud-hosted data, it also reduces the risk of your private network being compromised by outside attacks. Furthermore, a well-configured edge network can overcome congestion problems that might occur with devices and applications by rerouting traffic to the correct destinations and ensuring that your network is not overloaded.

Then there's the cost savings. By deploying devices on the edge and thereby offloading the processing and storage requirements to the edge, businesses can reduce the costs they would typically incur to purchase from cloud providers.
That said, not all edge networks are created equal, and a poorly configured edge can turn all these benefits into disadvantages.

First and foremost are the security risks. Businesses need to make sure their edge is ultra-secure and can respond to threat incidents emerging from different devices or locations. Secondly, without the correct knowledge and training, your IT team may quickly be overwhelmed by having to manage the multitude of devices, locations, and applications that make up the edge.

A third challenge is the upfront cost. Implementing edge networking into your business can be expensive as it requires the purchase and deployment of suitable devices and systems that achieve the desired aims without sacrificing security.

Enter the automated edge

Unsurprisingly, the technology behind edge networking is evolving all the time, and a recent advancement is the automated edge. In simplified terms, the automated edge is intelligence that is embedded into edge devices which takes care of networking tasks like configuration, responsiveness, provisioning, and even monitoring all by itself.

As your daily operations shift and change, it will automatically optimise network performance by intelligently steering traffic through different pathways to reduce lag time and interruptions while providing greater reliability and security.

Best of all, the automated edge can work hand-in-glove with your generative AI models to improve connectivity and real-time decision making from different devices, locations, and applications. This not only accelerates the analysis of your data close to the source, but also speeds up customer interactions and provides further opportunities for growth and innovation.

Additionally, if your business relies heavily on low latency – which most businesses do – then your IT team will no longer have to constantly manage any blockages in your network and then figure out the best solution. The automated edge does it for you.

The simple solution to edge automation

The sheer complexity of the automated edge has led many companies to seek out partnerships with network-as-a-service providers to give them a fast, flexible, and competitive advantage. Network as a service, or NaaS for short, provides companies with an efficient end-to-end solution in the operational management and performance of their networks on a subscription basis.

The beauty of this business model is that removes all the complexity. A NaaS provider helps you to build your own private network on your own terms, one that can be scaled and configured to meet your needs. It also takes care of security issues and protects your network from attacks through constant monitoring and early detection.

But crucially, a tried and tested NaaS provider will have already embedded their platform with the latest automated edge capabilities to interact and interface with all manner of edge devices and applications. This not only allows you to deploy new technology tools safely and efficiently, but also frees up your IT team to concentrate on other mission-critical tasks.

As for network management, your business will have total visibility of your network infrastructure from a single user-friendly dashboard, allowing you switch-up performance and agility on demand. Meanwhile, all your network maintenance concerns are taken care of 24/7 by an expert team of engineers.

If businesses truly want to harness the potential of 'the internet of things', they must first consider moving to the edge. Indeed, by laying the foundational groundwork today for what is surely to come tomorrow, they can take full advantage of future advancements in network edge innovation.

Accelerating the circular economy through software

Anders Brejner, Investment Director and Enabling Solutions Lead at Circularity Capital, discusses the growing corporate demand for digital solutions which can unlock the commercial advantages of the circular economy at scale.

IN THE ONGOING PUSH for efficiency and productivity, companies are increasingly turning to data and software driven insights. This doesn't just serve the purpose of closed system efficiency, but is an enabler of what we believe is the next frontier; the transition to more sustainable, circular way of operating.

We are now in a rapidly evolving regulatory environment with increasing focus on 'social licence to operate', where corporates are increasingly incentivised to provide governments, shareholders, employees and consumers with accurate and timely information about their emissions and supply chain sustainability[1]. Companies can benefit greatly by proving that necessary changes are being made to reduce their negative externalities to the world, which drives a multitude of positive effects for the businesses themself: higher revenues through volume and higher prices; employee attraction and retention; and better access to high quality capital

Aside from greenhouse gas emissions, supply chains are increasingly under scruitiny for their wider impacts on people, the environment and the economy. Companies are increasinly looking to implement and report on a variety of measures to improve supply chain sustainability, with mechanisms like traceability of material, inventory auditing, environment impact assessments (LCAs), circularity, fair treatment of workers, waste management, and energy and water consumption all needing to be tracked and reported on.

If the results do not offer enough evidence to assure stakeholders of the company's sustainability progress, the data can be used to find and plug in the gaps.

This is where the strength of good data management lies. With such vast streams of sustainability information available, corporates need a way to aggregate and evaluate data to fully unlock its full potential.

It's clear to see that the circular economy provides a strong framework for decoupling business growth from resource constraints, enhancing resource productivity and driving competitive advantage. It also highlights a subset of business models which are enabling this transition and can generate premium returns for investors

A digital-first approach

A growing number of technology solutions are making it increasingly possible to collect, sort and analyse data at a faster rate[2]. It's only with the data consistency and transparency offered by these services that business will be able to effectively execute the transition from today's linear, carbon intensive, take-make-dispose methods of production and consumption and into a more sustainable, circular economy model.

And this is a viewpoint increasingly shared amongst business leaders. In its 2023 State of Corporate ESG report, the Tomson Reuters Institute found that 71% of C-suite and functional leaders anticipate a growing significance of ESG in business performance, and the use of digital solutions to provide fresh insights was found to be one of three main priorities for businesses, the other two being AI and global regulations.

At Circularity, we have invested in several companies that leverage technology to provide this transparency to their customers:

- Trustrace provides SaaS solutions that help leading brands like Adidas in the fashion and textiles industry to create full traceability of products; from sourced material to finished product.
- Winnow provides AI technology for commercial kitchens to help lower food waste by measuring waste streams and drive optimisation in procurement.
- CEMAsys provides SaaS and consultancy services to provide companies with a granular understanding of their carbon footprint, as well as insight surrounding how to reduce it.

Growth-stage capital funding

When we founded Circularity Capital in 2015, we did so with the firm conviction that the entrepreneurs of businesses like Trustrace, Winnow and CEMAsys, who are developing the data-driven innovations to make the circular transition a reality, deserve a specialist investor with the right knowledge and network to unlock their full potential. While there is significant VC funding available, there is limited access to growth equity to help take these business to the next level.

We have worked hard to develop a firm with the right capabilities to make this a reality and are currently deploying our second dedicated circular economy private growth-equity fund – it is the largest of its kind globally. Our portfolio already includes a diverse range of leading circular businesses across Europe, but our ambition is to further grow this investment base by supporting leading, innovative, circular businesses where we can add value as a domain expert investor.

It's clear to see that the circular economy provides a strong framework for decoupling business growth from resource constraints, enhancing resource productivity and driving competitive advantage. It also highlights a subset of business models which are enabling this transition and can generate premium returns for investors. Indeed, circular economy thinking will drive industry for years to come.

The supply chain is set to experience rapid change over the coming years. At Circularity Capital, we're looking forward to playing a leading role in the transition towards a more resource-efficient future utilising the power of data.

FURTHER READING / REFERENCE

➤ 1. https://www.virginmediao2business.co.uk/sustainability/esg-survey-results/
➤ 2. https://www.newscientist.com/article/2376512-deepmind-ais-new-way-to-sort-objects-could-speed-up-global-computing/

Leadership 4.0: The tech-powered way in the modern working world

The digital revolution has fundamentally reshaped the business landscape. Traditional leadership styles, characterised by rigid hierarchies and top-down decision-making, are proving increasingly ineffective in this dynamic environment. To thrive in the age of constant disruption, a new leadership paradigm is emerging... Leadership 4.0.

BY DAVID MALAN, SALES DIRECTOR, UK AND IRELAND, DOCUWARE

LEADERSHIP 4.0 reflects the realities of Industry 4.0, a world marked by interconnectedness, automation and the influence of exciting technologies such as artificial intelligence (AI). This leadership style prioritises agility, collaboration and a focus on human potential. Leaders in this new era act as facilitators and coaches, empowering teams to innovate and solve problems collectively.

Building a culture of collaboration

Leadership 4.0 relies on effective technology integration. Leaders must carefully evaluate and implement the tools that support collaboration, communication and knowledge management. Cloud-based platforms can facilitate real-time communication, project management and knowledge sharing, regardless of location. Data analysis, powered by big data and analytics tools, provides valuable insights into everything from customer behaviour and market trends to team performance. This empowers leaders to make data-driven decisions, optimise processes and ultimately achieve better results. A Document Management System (DMS) centralises document storage, streamlines workflows and facilitates secure information sharing. This is ever so important for fostering transparency and collaboration within an organisation.

While technology is a powerful driver of Leadership 4.0, the human element remains irreplaceable. Leaders must remember that AI and automation tools are there to augment human capabilities, not replace them. The human touch is essential for tasks that require creativity, critical thinking, complex problem-solving and emotional intelligence. Business leaders play a vital role in fostering a culture of human-machine collaboration, where technology empowers employees to work smarter and achieve better results. Additionally, soft skills like empathy, effective communication and the ability to build trust are crucial for motivating and inspiring teams in a dynamic and ever-changing working environment.

Redefining success in the workplace

At the heart of Leadership 4.0 lies a shift towards networked thinking and action. Information silos

are broken down and replaced by a culture of collaboration that transcends traditional departmental boundaries, from sales and marketing, to IT and finance. Teams can use new tech tools to work together seamlessly and achieve shared goals and allow information to flow as needed across an organisation.

Agility and adaptability are paramount for modern businesses. Leaders must be able to react swiftly to changing market conditions and customer demands. This requires a willingness to experiment, embrace new technologies and continuously learn. Leaders must foster a culture of innovation and encourage calculated risks to stay ahead of the curve.

Empowerment and participation are central to Leadership 4.0. Employees are encouraged to take ownership of their work and actively participate in decision-making processes. This fosters a sense of responsibility and ownership, motivation and increased engagement. When employees feel valued and heard, they are more likely to contribute their best work, leading to a more positive and successful work environment for all.

Embracing a digital transformation

Leaders must champion the development of digital literacy within their teams to ensure everyone can leverage the power of new tools and platforms. Building digital skills empowers employees and allows them to excel in the ever-evolving digital age. While Leadership 4.0 offers significant advantages, there are also challenges to consider. Traditional mindsets can create resistance to new leadership styles. Therefore, business leaders must be adept at communication, persuasion and change management to navigate this challenge.

Shifting to a culture of openness, collaboration and transparency may require significant cultural change within an organisation. Technology that replaces repetitive manual tasks can be hard for some employees to trust. In geographically dispersed teams, maintaining clear communication can be a hurdle. Leaders must prioritise tech tools that enable effective communication across teams, departments and borders.

The road to Leadership 4.0 is an exciting one, If you're looking to empower your teams, embrace innovation and thrive in the digital age, we're here to help. At DocuWare, we offer technology solutions designed to support Leadership 4.0 principles.

Whether you need to bolster collaboration with cloud-based platforms, leverage data insights for better decision-making or streamline workflows across your organisation, we have the tools and expertise to empower your transformation.