DW

DIGITALISATION WORLD

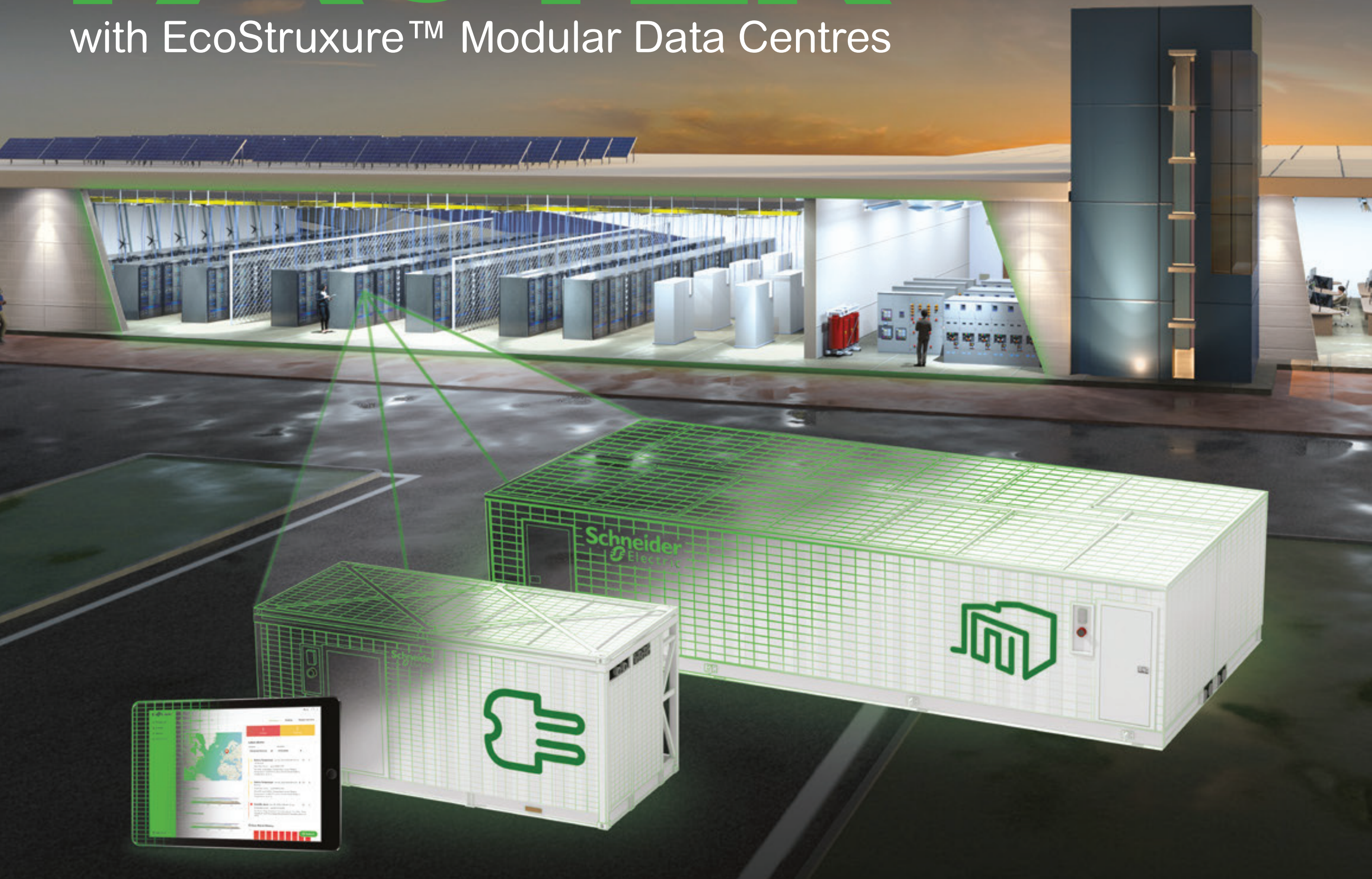
MODERN ENTERPRISE IT - FROM THE EDGE TO THE CORE TO THE CLOUD

ISSUE V 2025

AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

DIGITALISATIONWORLD.COM

OPTIMISING THE AI DATA CENTRE OPPORTUNITY


Schneider Electric

VIEWPOINT

BY PHIL ALSOP
EDITOR

AI – the jury is still out

NO APOLOGIES for returning to the hottest topic since hot cakes were leaving the bakery at incredible speed – AI continues to dominate. And when I say dominate, I am not just talking about the IT world, but the world, full stop. And when I say the world, full stop, I mean that, without in any way wishing to marginalize the sadly many horrendous events which have been witnessed across the globe over the past few years, AI's power for good and evil (sorry if it sounds like a line from a Batman movie) is off the charts when compared to anything else.

Don't believe me? Well, the wars, famines and weather extremes which are claiming so many lives may be front and centre, but, in the cyber world the disruption is already just as intense and, with the continuing development of AI, likely to get far more so. No, you won't see people fire up their laptops and suddenly keel over, struck dead. What you will see and, indeed, are already seeing, is 'AI-inspired' misinformation on such a huge scale that simmering resentments and anger are cultivated to boil over into violence. As to where this ends, who knows?

Additionally, the already massive numbers of cybersecurity attacks, many of which are state-sponsored, on governments and big businesses, have already caused much financial havoc. And it doesn't require much imagination to understand that, thanks to AI, these activities are only going to escalate further in terms of numbers and sophistication (a post-quantum security discussion anybody?!). We are surely only months or a year or so away from a whole government being brought to a virtual, and, therefore, actual, stand still, as the bad actors manage to compromise various data centres and IT systems to the extent that nothing works. One only has to think of the panic and chaos induced by the recent power outage in southern Europe to begin to understand where this might be headed.

Well, that's the glass half-empty bit – or maybe the dregs of the glass to be more accurate.

Many folks are quick to point to the many potential benefits of AI, alongside what is has already achieved. I will resist moving into the realms of ethics and moral philosophy, but simply state that, when it comes to healthcare, for example, the idea of having better, healthier and longer lives for us as individuals sounds amazing, but if this means more and more stress being put on the world's finite resources, where does it end…

Apologies if this all sounds a little bit gloomy – and I haven't even mentioned the many predictions as to how many jobs AI will make redundant. And, yes, I am a user of AI, so I am on no moral crusade to ban its use.

However, I am fairly confident that, without a similar attitude to AI regulation as currently exists, say, for nuclear weapons – and I am aware how crazy this might sound to many – then a future of AI without boundaries is not one that has much appeal.

In the mean time, I will content myself with chuckling at all those organisations and individuals who trumpet unchecked capitalism, letting the market decide, and the freedoms of AI, until they are outraged that their opponents are using the same beliefs and tools to do very different things. We live in very strange times indeed.

Let us hope that as many of us as possible come out on the right side of the not so delicately balanced AI equation - which all comes down to how the technology is used, not the technology itself.

CONTENTS

DW DIGITALISATION WORLD

NEWS

09

DIGITALISATION WORLD

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

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

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

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

Publisher
Jackie Cannon
+44 (0)1923 690215
jackie.cannon@angelbc.com

Circulation & Subscriptions
+44 (0)1923 690214
circ@angelbc.com

Directors
Scott Adams: CTO
Sukhi Bhadal: CEO

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.

The paper used within this magazine is produced by chain of custody certified manufacturers, guaranteeing sustainable sourcing. ISSN 2396-9016 (Online)

IT teams are losing visibility

New industry report highlights growing SaaS waste, persisting audit costs and evolving priorities as ITAM teams navigate increasing financial scrutiny.

FLEXERA has released the Flexera 2025 State of ITAM Report, which reveals a concerning decline in complete visibility across the technology stack - down to 43% from 47% year-over-year.

Yet, as pressure mounts to optimise costs, the collaboration of IT asset management (ITAM) with cloud (44%) and FinOps (38%) teams is on the rise, suggesting that ITAM teams are increasingly working across organisational silos to address comprehensive visibility challenges, increase financial accountability and drive operational efficiency.

Flexera's annual report surveys global IT professionals to explore how the evolution of ITAM, FinOps, security, software asset management (SAM) and hardware asset management (HAM) teams influences the value they deliver. It also examines IT investment trends across public, hybrid, and SaaS technologies.

"Complete visibility across IT assets is foundational to every good technology decision," said Becky Trevino, Chief Product Officer at Flexera. "The fact that it's slipping at a time when organisations are under intense pressure to rationalise costs is a real concern. You can't optimise what you can't see and without clear insight into the entire technology stack, it's nearly impossible to eliminate waste, ensure compliance, or make cost-effective investment decisions.

This year's report showcases why the collaboration between ITAM and FinOps is no longer optional – it's a strategic imperative."

Highlights from the latest Flexera State of ITAM Report include:

- **Minimising SaaS sprawl is an increasing imperative:** Thirty-five percent of respondents say SaaS waste has increased over the past year, suggesting that the financial impact of underutilised SaaS subscriptions is taking a toll on budgets. In addition, SAM professionals are doubling down on SaaS oversight, with 59% actively tracking usage and 56% rightsizing contracts and subscriptions to eliminate unnecessary spend.
- **Software use rights take the spotlight:** The report also highlights a dramatic rise in the challenge of managing software use rights—now ranked as the number one concern for SAM teams, up from sixth place just a year ago. This surge is largely attributed to the growing complexity of cloud-based licensing models and the rapid migration of enterprise resources to cloud environments.
- **Audits still plague organisations (and their bottom line):** Nearly half (45%) of surveyed organisations report spending over $1 million on software audits over the past three years, a figure one percentage point less than 2024. Twenty-three percent of organisations spent more than $5 million on audits in 2025, a slight increase from 2024. The findings suggest that the intricacies of software use rights and the continued shift to the cloud are keeping audit defence high on the agenda of IT teams.
- Microsoft continues audit streak: Half of respondents said Microsoft audited their organisation in the past three years. The tech giant has remained at the top of this list for the past several reports, followed closely by IBM (37%). There was a slight increase in audits reported from SAP (32%) and ServiceNow (21%) compared to last year's findings. Adobe (24%) remained unchanged, but Oracle decreased from 31% to 24% and Salesforce dropped from 25% to 20% year over year.

This year's findings underscore the urgent need for smarter, more agile SAM strategies as organisations strive to balance innovation with fiscal responsibility.

"The role of ITAM is shifting from operational to transformational," said Phil Perfetti, senior product marketing manager at Flexera.

"While visibility into cloud licenses is gradually improving, the complexity of managing hybrid IT environments is also increasing, and any serious blind spots are a problem that modern organisations can no longer afford."

As AI accelerates, human leadership becomes more essential than ever

The Corporate Governance Institute stresses that leaders must champion technological adoption and be at the forefront of the transition to a workplace shaped by intelligent automation.

IN THE next three years, artificial intelligence (AI) is set to drive unprecedented change across every sector. But as businesses race to adopt new technologies, one truth remains clear: the organisations that will thrive are those that double down on what makes them human.

The World Economic Forum's Future of Jobs Report highlights that 77% of leaders believe there is a need for reskilling and upskilling existing workers to better work alongside AI. According to Ciaran Bollard, CEO of The Corporate Governance Institute, a new leadership perspective is emerging , one that values empathy, creativity, critical thinking, and emotional intelligence as essential skills in the age of automation.

"Successfully integrating AI isn't just a technical challenge, it's a leadership one. Many digital transformation efforts fail not because of the technology itself, but because of a lack of clear communication, poor vision, and weakened organisational cohesion. These risks are only amplified when AI enters the equation."

To navigate the seismic changes brought about by AI, leaders must go beyond the technical implementation and focus on the human side of transformation. Bollard continues: "That means setting a clear, organisation-wide vision for how AI will be used, communicating transparently with employees, and offering both emotional and practical support throughout the journey. We must reinforce a shared sense of purpose, show how AI supports rather than replaces human contributions, and honour the legacy processes that got us here, while encouraging a mindset shift toward what's next.

"Crucially, we also need to invest in personalised upskilling and development to ensure every employee is equipped for the future. Leadership in the age of AI starts with empathy, clarity, and inclusion."

The stakes couldn't be higher. Studies suggest that up to 300 million jobs could be displaced by AI by 2030, with 9–20% of the global workforce expected to undergo significant change within just five years.

Technical debt stifling path to AI adoption

TECHNICAL DEBT and an over-reliance on outdated legacy systems and applications is blocking enterprise adoption of more innovative technologies like artificial intelligence (AI), according to new research from Pegasystems.

The study, conducted with research firm Savanta, was unveiled at PegaWorld®, the company's annual conference in Las Vegas. It surveyed more than 500 IT decision makers across enterprises worldwide on the challenges caused by technical debt and the progress in modernizing legacy technology.

The study found that two in three (68%) respondents say legacy systems and applications are preventing their organization from fully embracing more modern technologies. An overwhelming majority (88%) are also concerned about how their technical debt impacts their ability to keep pace with more agile, innovative competitors – with one in three (29%) indicating either 'clear' or 'significant' concern. More than half (57%) even acknowledge their reliance on legacy systems 'likely' or 'highly likely' causes customers to defect due to the resulting poor experiences.

Other findings from the research include:

- **Legacy dependency:** Almost half (48%) say they can't stop supporting their legacy applications – despite wanting to – because the systems are still business critical. Almost half (47%) say their oldest legacy application is between 11-20 years old, while more than one in ten (16%) run apps between 21-30 years old.
- **Legacy ineffectiveness:** Two thirds (68%) of respondents say legacy systems are preventing their organization from operating as effectively as possible, citing time spent on maintenance (44%), the siloed nature of disconnected systems, and the cost of maintenance (both 37%) as the leading contributing factors. Just 7% feel legacy applications caused no problems for their business whatsoever.

The customer does not always come first: Three quarters (74%) of respondents agree their business prioritizes investments that improve profitability instead of ways to improve customer experience, such as technologies to help modernize legacy applications.

AI underdelivers at work

GoTo has released a new research report: The Pulse of Work in 2025: Trends, Truths, and the Practicality of AI.

THE REPORT summarises the findings of a survey of 2,500 global employees and IT leaders on AI use and sentiment, conducted in partnership with research firm Workplace Intelligence. Among the study's key findings: despite widespread anticipation about AI's positive impact on workforce productivity, most employees feel they were overpromised on its potential. In fact, 62% believe AI has been significantly overhyped.

However, this is likely because employees aren't making the most of what these tools have to offer. The majority (86%) admit they're not using AI tools to their full potential, and 82% say they aren't very familiar with how AI can be used practically in their day-to-day work.

All told, employees estimate that they're spending 2.6 hours a day — or 13 hours per week — on tasks that could be handled by AI. This means that in the U.S. alone, businesses could be missing out on more than $2.9 trillion annually in greater efficiency.

"Employees are already using AI and are seeing clear productivity gains, yet despite these benefits, our latest research shows people still view AI as overhyped.

While many recognise its value, they don't yet see it as the revolutionary change they were promised. This gap likely exists because many workers admit they aren't realising AI's full potential or don't know how to apply it in practical ways," said Rich Veldran, CEO of GoTo. "The solution is clear: companies must go beyond just providing access to AI by ensuring employees have both the right tools and the right education. By equipping teams with effective training and clear guidelines, organisations can empower their workforce to unlock the true, transformational impact of AI."

Other key findings include:

- AI is handling some tasks for employees — just not the ones their bosses think: Instead of using AI to save themselves time in their day-to-day work, 54% of employees admit they've used it for sensitive tasks or high-stakes decision-making such as tasks requiring emotional intelligence (29%), tasks impacting safety (25%), and ethical or sensitive personnel actions (16%) — despite knowing they shouldn't. An alarming 77% of these workers also say they don't regret using AI for these tasks.
- Another potential reason for AI's underuse — employees don't trust the tools: 86% of employees aren't very confident in the accuracy and reliability of AI tools, and 76% say they often provide outputs that need to be refined or revised by users.
- Smaller companies are falling behind: At the smallest companies — those with 50 employees or less — just 59% of workers use AI, and 46% say they don't know how to use AI to save time or improve their work. At larger organisations, however, closer to 80% are using AI.

"Contrary to what you might think, it's not just older workers who are struggling to realise the benefits of AI tools," said Dan Schawbel, Managing Partner, Workplace Intelligence. "Younger workers also admit they're not using these tools to their full potential. In fact, 74% of Gen Z employees say they aren't very familiar with how to use AI practically in their day-to-day work. This highlights the importance of equipping all generations with the tools and education to use AI safely and effectively."

The research also describes solutions to help close the AI adoption gap:

- Give employees the tools they want: Employees say an AI virtual assistant (88%), AI tools that automate certain work tasks (86%), AI communication tools (83%), generative AI tools (81%), and an AI chat/messaging assistant to communicate with customers (73%), would be most valuable for them, but roughly only 4 out of 10 say their company offers these.
- Improve policies and training to prevent AI misuse: Just 45% of IT leaders say their company has an AI policy in place. Both employees (81%) and IT leaders (71%) believe AI tools need better instructions and guardrails for proper usage. 87% of employees also feel most workers are not being trained properly to use AI tools.
- Be purposeful about AI implementation and ROI measurement: At companies using AI, 21% of IT leaders admit their company is adopting AI or buying AI tools just because they think they should — not after careful consideration or with a clear plan in mind. What's more, nearly half (49%) of IT leaders say their company isn't measuring the ROI of AI tools very well.
- Recognise that a small investment can have a major impact: 77% of IT leaders say their company would only need to spend an extra $20/month or less per employee on AI tools to save each employee an additional one hour a day in greater efficiency.

A major infrastructure shift is underway

AI could double the strain or solve it.

CISCO has released a new global study revealing a major architectural shift underway across enterprise networks. As AI assistants, agents, and data-driven workloads reshape how work gets done, they're creating faster, more dynamic, more latency-sensitive, and more complex network traffic.

Combined with the ubiquity of connected devices, 24/7 uptime demands, and intensifying security threats, these shifts are driving infrastructure to adapt and evolve.

The result: IT leaders are changing how they think about the network: what it is, what it enables, and how it protects the organization. The network they build today will decide the business they become tomorrow.

Six signals that an architectural shift is underway

- **The network has become a strategic priority:** 97% say a modernized network is critical to rolling out AI, IoT, and cloud. 91% of IT leaders plan to increase the share of their overall IT budget allocated to networking.
- **Secure networking is mission critical:** 98% say secure networking is important to their operations and growth; 61% say it's critical. 94% believe an improved network will enhance their cybersecurity posture.
- **AI intensifies demand for resilient networks:** 95% of IT leaders say a resilient network is critical, at a time when 77% faced major outages – driven largely by congestion, cyberattacks, and misconfigurations – adding up to $160B globally from just one severe disruption per business, per year.
- **Leaders look to AI to grow revenue:** 55% of IT leaders say a modernized network's greatest impact on revenue will come from deploying AI tools that automate and tailor customer journeys – enabling faster, more personalized experiences that can strengthen loyalty and drive growth.
- **AI is reshaping computing infrastructure:** 71% say their data centers can't yet meet today's AI demands, and 88% plan to expand capacity – on-prem, in the cloud, or both.
- **Leaders want to make networks smarter:** 98% say autonomous, AI-powered networks are essential to future growth – yet only 41% have deployed the intelligent capabilities – like segmentation, visibility, and control – to make their network adaptive.

"AI is changing everything — and infrastructure is at the heart of that reinvention. The network has powered every wave of digital transformation, accelerating the convergence of IoT, cloud, hybrid work, and defending against rising security threats," said Chintan Patel, CTO and Vice President Solutions Engineering, Cisco EMEA. "IT leaders know the network they build today will shape the business they become tomorrow. Those who act now will be the ones who lead in the AI era."

The Network is the Value: Modern Infrastructure Unlocking Growth and Savings

IT leaders are already delivering financial value from today's networks – largely by improving customer experiences (55%), boosting efficiency (52%), and enabling innovation (51%). But much of that value is at risk if it comes from infrastructure that hasn't been designed for AI or real-time scale.

To unlock the full growth and savings they expect, leaders have identified critical gaps they must close: siloed or partially integrated systems (58%), incomplete deployments (51%), and reliance on manual oversight (48%). Smarter, more secure, more adaptive networks are the business case for investment. Nearly 9 in 10 (89%) say improved networks will directly drive revenue, and almost everyone (93%) expects meaningful cost savings – driven by smarter operations, fewer outages, and lower energy use.

The C-suite is turning to IT leaders and partners to lead the architectural shift Cisco's recent research shows CEOs are aligned with IT leaders on the importance of infrastructure in the AI era. 97% are expanding the use of AI, and 78% rely on their CIO or CTO for investment decisions. But they also recognize the risk: 74% say outdated infrastructure is already holding back growth. As enterprise networks undergo a major architectural shift, the C-suite is backing their tech leaders to lead from the network – and 96% believe trusted partnerships will be critical to success.

Focus on the individuals affected, not the number of breaches

30% of incidents account for 80% of exposed personal data, says Huntsman Security.

PREVENTING just a third of reportable data security incidents could protect nearly 80% of breach victims in the UK and Australia, according to new analysis from Huntsman Security. The company's review of regulator data shows that a relatively small number of attacks and errors, most of which could be mitigated by best practice security controls, are the cause of millions of individuals' personal information being compromised each year.

The analysis is based on the UK Information Commissioner's Office's (ICO) data on security incidents and a Freedom of Information request to the Office of the Australian Information Commissioner (OAIC).

Huntsman found that just 29% of data security incidents in the UK and 32% of reported data breaches in Australia were responsible for the vast majority of compromised data records, affecting tens of millions of individuals. The most common causes of breaches were familiar and persistent, such as phishing, malware and inappropriate access to data.

The data highlights the security challenges faced by organisations and the critical importance of getting the basics right. By focusing on these particular incident types and embedding basic, routine cyber security processes into their "business as usual" operations, security teams can more effectively monitor their systems and identify any potential attacks.

UK: A small number of breaches, a large number of victims

Huntsman Security's review of UK ICO data for 2024 shows that just 2,817 data security incidents, or less than a third (29%) of the 9,654 where a cause could be identified, were linked to the specific threat vectors of brute force attacks, malware, phishing, ransomware, or

system misconfigurations. These incidents were responsible for nearly 80% of all individuals affected by a data security incident that year, with 13.9 million people impacted out of a total of 17.6 million.

These 2,817 incidents also made up around 90% of all cyber-related data security incidents, underlining the importance of prioritising controls that protect against them. Many of these attacks are targeted, and therefore more likely to compromise high-value data, including health records, financial information and identity documents, thereby increasing the risk of data loss for both individuals and organisations.

Australia: A high-impact breach landscape with slow detection times

In Australia, the picture is similar. Just 1,188 incidents (32% of all eligible data breaches reported between 2022 and 2024), that involved brute-force attacks, phishing, malware, ransomware, hacking, and unauthorised access, were responsible for 77% of all compromised records.

Looking at the broader picture, OAIC data shows that while malicious or criminal attacks accounted for just 62% of all eligible data breaches (2,312 out of 3,742), they were responsible for a staggering 98% of affected individuals — 203.5 million data records out of a total 207 million.

A key concern highlighted in the Australian data is detection and response time. On average, it took organisations 48 days to identify these breaches, and in total 86 days before reporting them to the OAIC. This could prolong the period of risk exposure for affected individuals and compound the reputational and regulatory impact for the organisation.

"While it's unrealistic to expect organisations to prevent every breach, the data shows that implementing some basic controls could really make a difference," said Peter Woollacott, CEO at Huntsman Security. "Adhering to established security frameworks like NIST or the ACSC Essential Eight can dramatically reduce, not only the number of incidents, but – more importantly –the number of people affected by those incidents overall. Putting in place baseline controls such as effective and timely patching, multi factor authentication, user application hardening and regular backups can make the world of difference when it comes to effective cyber security."

AI is now the leading security concern

AI surpasses ransomware as the top concern, as organizations navigate the double-edged sword of innovation and risk.

ARCTIC WOLF has published findings from its State of Cybersecurity: 2025 Trends Report, offering insights from a global survey of more than 1,200 senior IT and cybersecurity decision-makers across 15 countries. Conducted by Sapio Research, the report captures the realities, risks, and readiness strategies shaping the modern security landscape.

The research reveals a shifting risk environment, with artificial intelligence (AI) and large language models (LLMs) emerging as the top concern for security leaders.

For the first time, AI, including tools such as LLMs, has overtaken ransomware as the most pressing issue. While organizations are making substantial cybersecurity investments, the report also highlights persistent challenges including limited visibility, outdated incident response plans, and budget pressures.

Key findings from the report include:
AI Surpasses Ransomware as the Top Concern: 29% of security leaders cited AI, LLMs, and privacy issues as their number one concern, surpassing ransomware, malware, and data extortion (21%).

Breaches are Common and Transparency is Improving: 52% of respondents confirmed a breach in the past year (up from 48%), with 97% of known breaches disclosed. This indicates progress in regulatory compliance and incident transparency.
Significant Attacks Remain Widespread: 70% of organizations experienced at least one significant cyber attack in 2024, with malware and business email compromise being the most common.

Professional Ransomware Negotiators Reduce Payouts: Among those hit by ransomware, 76% paid. Of those, 90% engaged a professional negotiator, which led to reduced payments in more than half of the cases.
Endpoint Tools Are Widely Deployed but Visibility Lags: While 84% use next-generation endpoint security solutions, only 40% say they have 100% coverage and expect to maintain it.

“Arctic Wolf’s 2025 Trends Report offers a telling snapshot of how security leaders are thinking,” said Dan Schiappa, president, Technology and Services, Arctic Wolf. “AI’s rapid emergence is creating new uncertainty, not only in how attackers operate but also in how defenders must respond. At the same time, ransomware remains a persistent and costly threat. As organizations race to implement AI-powered tools, it is critical they also do not lose sight of core security fundamentals like patching vulnerabilities, implementing detection and response, and maintaining a current incident response plan.”

AI accelerates both attacks and defences, but critical security gaps persist

DELINEA has unveiled new research highlighting how ransomware attacks have continued to surge over the past year, despite fewer victims paying. Over two-thirds (69%) of organisations globally have fallen victim to ransomware, with 27% being hit more than once. Meanwhile, attackers are harnessing AI to automate, scale, and sharpen their operations.

Based on insights from over 1,000 IT and security leaders worldwide, the 2025 State of Ransomware Report reveals an increasingly volatile threat landscape driven by AI-powered attacks, stolen credentials, and Ransomware-as-a-Service (Raas). While only 57% of organisations paid ransoms, down from 76% in 2024, the frequency and impact of attacks continued to grow as threat actors turned to other tactics like extortion, with 85% of ransomware victims threatened with exposure.

“Ransomware has evolved into a shape-shifting, AI-enabled threat that no business can afford to underestimate,” said Art Gilliland, CEO at Delinea.

“In order to combat the sophistication of today’s attacks, organizations must fight AI with AI and embrace proactive, identity security strategies like zero trust architecture, Privileged Access Management, and continuous credential monitoring to stay ahead.”

The report highlights the growing role of AI on both sides of the ransomware equation. Threat actors are using AI to automate phishing, impersonate trusted individuals via deepfakes, and accelerate attacks. At the same time, defenders are increasingly relying on AI to detect and respond to threats faster, with 90% of organisations now using AI in their ransomware defence strategies – primarily within Security Operations Centres (64%), for analysing Indicators of Compromise (62%), and to prevent phishing (51%).

Despite 90% of executives expressing concern over ransomware threats, many organisations continue to fall short in essential security practices, with only 34% enforcing least privilege access controls and just 57% implementing application control measures. Most victims reported extended recovery times, with 75% taking up to two weeks to recover.

Addressing inequalities in AI access and training

The Adaptavist Group reveals workplace AI implementation is deepening inequalities, with discrepancies in access to AI tools and training affecting women's and lower earners' opportunities.

THE Adaptavist Group's recent Digital Etiquette report, 'Unlocking the AI Gates', highlights concerning trends in AI access and training. Released today, the study reveals the adoption of AI technologies exacerbate systemic inequalities in the workplace.

A survey of 4,000 knowledge workers across the UK, US, Germany, and Canada underscores that high earners are benefiting disproportionately from AI advancements. Those with high household incomes exceeding £100,000 were significantly more likely to receive comprehensive AI training over the last year compared to those earning £30,000 or less. Access to new AI tools and sufficient guidance come more readily to these high earners.

AI adoption offers significant gains in efficiency and job satisfaction although these gains are higher for those on higher incomes. However, the glaring disparities in access mean that lower earners and women risk being sidelined from new opportunities and advantages.

While 78% of high earners regularly access new AI tools, less than half of those on lower incomes experience the same privilege.

Training Gaps and Societal Implications

- 25% of lower earners lack adequate AI training.
- High earners report a 50% increase in job satisfaction from AI, compared to 14% among lower earners.

The research also identifies training disparities between large enterprises and small businesses, with smaller operations often receiving insufficient or no training. This points to an emerging divide that underlines the need for equitable AI training strategies. The study crucially illuminates the gender gap in AI education. Men consistently receive more formal AI training across all hierarchical levels compared to women, emphasizing a concerning trend that could result in further entrenched gender-based occupational inequalities.

The rise of AI in cybersecurity

SC2, renowned worldwide as a leading nonprofit member organization for cybersecurity professionals, recently unveiled its 2025 AI Adoption Pulse Survey. The survey aims to evaluate how AI security tools are being integrated across cybersecurity teams and their effects on efficiency, hiring, and job roles. Survey insights were gathered from 436 global cybersecurity experts working in organizations of varying sizes.

The survey reveals that AI's influence is reshaping operational modalities within the cybersecurity industry. Currently, 30% of cybersecurity professionals have incorporated AI security tools into their workflows. These tools are defined to include AI-enabled security solutions, generative AI, and agentic AI for autonomous actions. Encouragingly, 70% of those who have embraced AI tools report positive impacts on team effectiveness.

There's growing momentum towards adopting AI tools, with 42% of cybersecurity teams currently testing AI solutions.

Key areas showing the fastest positive operational impacts include:

- Network monitoring and intrusion detection: 60%
- Endpoint protection and response: 56%
- Vulnerability management: 50%
- Threat modeling: 45%
- Security testing: 43%

Among varying organization sizes, the largest firms lead with a 37% adoption rate, followed closely by mid-to-large and smaller organizations at 33%. In contrast, mid-sized and the smallest organizations show the lowest adoption rates, each at 20%. Notably, 23% of the smallest organizations have no immediate plans to pursue AI security tools.

Industries actively adopting or evaluating AI security tools include industrial enterprises (38%), IT services (36%), and the consumer sector (36%). The financial services (21%) and public sectors (16%) lag behind but show future inclinations towards evaluating AI tools.

The entry-level landscape is also being reshaped, with more than half of respondents believing that AI will diminish the demand for junior employees. Conversely, 31% view AI as a potential creator of new roles, enhancing early-career opportunities. Additionally, 44% state that AI has yet to influence their organization's recruitment strategies.

The adoption of AI security solutions necessitates a revision of roles and skill requirements, with 44% of professionals indicating changes are underway in their organizations to adapt to AI.

MANAGED SERVICES SUMMIT LONDON

10.09.2025

CONVENE
155 BISHOPSGATE LONDON

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

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

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

INDUSTRY INSIGHTS

Gain actionable knowledge from expert-led presentations focused on emerging technologies, market shifts, and the evolving role of MSPs in today's digital-first landscape. Understand what's next for cybersecurity, cloud strategy, and customer success.

BREAKOUT SESSIONS

Dive deeper into key areas with focused sessions tailored for technical leaders, sales professionals, and business strategists. These intimate, topic-driven discussions offer practical guidance and real-world solutions.

NETWORKING OPPORTUNITIES

Forge meaningful connections with fellow MSPs, technology vendors, and channel leaders. The summit's structure encourages open dialogue, peer learning, and opportunities to form long-term business relationships.

INTERACTIVE EXPERIENCES

Participate in demos, discover real-world case studies, and interactive panels designed to turn insights into action. These sessions let you explore solutions up close and ask the questions that matter most to your business.

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
Arjan Drayton-Chana arjan.dc@iteuropa.com
+44 (0)7516 501193

https://london.managedservicessummit.com

Angel Business Communications · IT EUROPA · ANGEL EVENTS

Optimising the AI data centre opportunity

David Mann, T&E LoB Category Management Leader for Europe & France at Schneider Electric, discusses the ways in which the AI revolution is changing the data centre 'rules' – requiring ever higher densities of servers and power alongside the anticipated development of AI applications at the edge. David explains some of the technology solutions which Schneider Electric has developed to address the differing demands of both high-density, hyperscale and relatively small scale, distributed data centre infrastructure.

DW: *Hybrid IT infrastructure seems to have become the default approach to digital transformation. Is that fair to say?*

DM: Yeah, I'd say it has. Hybrid IT infrastructure has pretty much become the default for digital transformation. And we can see this with the shift of data centre infrastructure management software. Businesses can no longer rely on traditional centralised data centres.

We're seeing a gradual shift to the mix, including on premise, co-location, cloud, and edge computing. Those all help companies optimise performance, scalability, and achieve better cost efficiencies at the same time. If I think about the way that complex and distributed environments demand resiliency, that plays a key part in the continued evolution of DCIM. If we take something like security, for instance, with hybrid IT, cybersecurity risks naturally increase. DCIM addresses that elevated risk with independent cybersecurity certifications, automatic firmware updates, and access control. It gives an operator the peace of mind they're looking for to feel secure.

DW: *Okay, that's where we are now, and everyone's got fairly used to adjusting to the requirements around hybrid IT. Then along comes AI, which has driven a coach and horses through all received wisdom up to this point. The rules are changed. I guess everyone is aware that AI is having this impact, but perhaps you can articulate the ways in which it is changing the rules, certainly around the data centre and infrastructure?*

DM: I can give you some examples, actually. AI is already starting to dramatically reshape everything about IT infrastructure. Just as organisations, were trying to get to grips with the complexities of hybrid IT this new AI-driven workload environment, particularly generative AI, is completely changing the rules again. AI naturally requires significantly higher rack densities. It wasn't that long ago, actually, that one of our best-selling

server racks was a pretty standard 42U height, 600 millimetre wide, 10, 70 millimetre deep rack. It was probably running somewhere between 4 and 10 kilowatts at the absolute outside of a co-location provider, and cooling could have probably been a bit of an afterthought.

Now with AI, we're seeing opportunities asking for 50 to 100 kilowatts set-ups per rack to cater for these AI-optimized server designs and the specialised chipsets they're using. So naturally, this is driving the conversation of power and cooling to completely different levels, well beyond what traditional air cooling can handle as a good example. So CDUs, chilled water loops are emerging now as the go-to solution in AI-driven data centres.

And AI adoption is not really a matter of if, but when. I mean, good investment in hybrid IT strategies, advanced cooling, potentially deploying modular data centres are now all serious considerations that businesses are having to make.

DW: *Are people able to easily and sensibly repurpose legacy data centres to take advantage of what you've described, racks and racks of high-density servers? Or are we mainly talking about greenfield or brownfield sites, where they're starting with a reasonably blank piece of paper and, therefore, they can build the best infrastructure for this AI requirement?*

DM: Funny enough, the one thing you hear more about actually is getting a connection. Because of the high power requirements, at a couple of the events I've been to most recently the biggest topic of discussion is where to position these new data centres if you can actually build them in the first place. There seems to be a bit of a shift, actually, to try and use some very unorthodox buildings that have already got a power connection, actually.

Something where there's already power availability there, I know of one example where they're modifying an old Victorian premises in central London to accommodate a data centre, because the wait time to actually get a new connection onto the grid for the power that some of these loads need is just too for many of these new companies.

If you've got the space and you've got the electrical connection, you can probably upgrade into taller racks to make better use of your space. And obviously, as long as you've got enough power coming into the building, you can probably make it work. We actually have some great containment solutions to allow for the cooling that's needed

Also, at a recent event held in London, there was talk about trying to position some of these data centres near some of the renewable energy sources around the UK. The only downside to that is a lot of our renewable energy comes from the highlands of Scotland and in Wales. So, it's not overly close to maybe where the main user base is.

In terms of the buildings themselves, there seems to be a lot of adaptation that's happening at the moment to try and make them fit where they can. In terms of reusing some of the existing physical architecture, like the racks, this can be a bit tricky, actually, because some of the original racks that have been deployed aren't deep enough to allow for some of these new AI servers. That's always a bit of a challenge, actually, because some of the new servers that are coming to market now, particularly the generative AI inference servers, are enormously long. You can't fit these into a standard rack.

DW: *With all that's going on, you mentioned that power availability is maybe the main bottleneck, but there is also a problem with data centre capacity. The legacy facilities maybe need to be upgraded or can just carry on hosting traditional applications. But there's also a lot of construction going on - how easy it is to get the capacity for AI?*

DM: If you've got the space and you've got the electrical connection, you can probably upgrade into taller racks to make better use of your space. And obviously, as long as you've got enough power coming into the building, you can probably make it work. We actually have some great containment solutions to allow for the cooling that's needed. There is certainly a shift in the cooling, as I mentioned, away from airflow cooling more into chilled water. So, potentially there's a couple of changes to the actual physical infrastructure you're going to need to do to adapt.

But I think you can modify some of the space you've got to fit some of the new requirements in. I suppose you have to adapt, don't you? Because the cost of building an entirely new site can be extremely high. And there's a significant amount of time to do this as well - you might miss the opportunity.

DW: *We've talked about the large data centres required to house all these racks of high density servers, supporting hardware and the like – there's talk of building gigawatt factories for AI. Before AI, all the talk was about edge data centres and IoT and all the fantastic things were going to happen here. But not a great deal happened. However, now, once the AI large language models have done their stuff, then all the AI inferencing and then the actual AI applications are going to be rolled out. So, there's going to be a big development alongside the huge AI data centres of a lot more localised, edge infrastructure?*

DM: I think this is absolutely correct. At the moment, AI is still in the training mode. As soon as the inference models starts coming to fruition, it's going to move a lot of the emphasis back on-premise again. Those hybrid IT strategies we were talking about before become certainly very prevalent for businesses.

In the future, once companies know how to make AI work for them, they'll absolutely understand the benefits of bringing that on-premise IT back, the low latency – most importantly, the low latency that you'll need for AI, especially with the rise of IoT, this is going to be

very, very important for businesses of all sizes.

DW: *So, at one level, we have the need for data centre infrastructure that can help address the high density requirements we talked about for AI. And I believe this is where Schneider Electric's white space portfolio has a role to play. Perhaps you can give us a bit more of an insight as to what it is?*

DM: Less than a decade ago, our top selling rack was actually just a standard 42U height server rack. Our next generation of racks are being built to accommodate these new AI workloads running in very powerful servers that are actually exceptionally heavy and they're really long - we've needed to adapt. Our APC Net Shelter generation 2 racks that we brought to market last year, and we're bringing out a few more of these this year as well, provide at least an additional 25 % weight capacity advantage over our previous generation. And we've also ramped up the air perforation through the doors from what was 69% to 80%, allowing for improved airflow and better cooling.

Our most popular options are now increasing the width as well as being much deeper. Server vendors prefer larger rack heights to maximise the amount of GPUs per server per rack.

This year, you'll start seeing from us that rack heights are going up to 52U, with our current rack portfolio already having 45 and 48U rack heights, which are increasingly popular. A 52U rack, by the way, is pretty much a sight to behold! It looks absolutely enormous next to a standard 42U height rack.

As mentioned previously, widths are also increasing. Standard options of 750 and 800 millimetre are increasingly being requested. And 1200 millimetre deep racks are now available on our standard platform in both black and white. Specifically for AI applications, we're bringing on to the market an exciting roll-on roll-off high strength rack in both 48 and 52U heights that can go as deep as about 1470 millimetres. This should be available in the middle of the year, and it's going to be able to take a static load of nearly 1,930 kilogrammes and a rolling load or a dynamic load of around about 1,590 kilogrammes.

For perspective, this dynamic load is actually 500 kilogrammes more than standard racks typically offer. It comes supplied with all the required anti-shock packaging and everything required for server integrators to pretty much build, configure and test racks fully off-site before being delivered ready to go

DW: *In terms of the more localised, smaller scale data centre infrastructure required for edge, clearly you're well known for your UPS solutions and the smart UPS in particular. And this is an ideal solution in terms of providing network power protection in the more regionalised, localised edge environments?*

DM: For edge or distributed IT, however you want to describe it, these single-phase platforms are absolutely perfect. We have single-phase offerings all the way up to 20 kilowatts. We've got a variety of solutions in our portfolio. Most people know APC for single-phase UPS, more than anything else. We have a very strong portfolio that's we're always increasing. We've moved into the likes of lithium-ion technology that brings significant benefits, especially for smaller distributed IT branch networks or similar, where you've got multiple assets across the field that are increasingly difficult to manage and maintain.

You need all of these connected to a single software platform, so this connects into our Schneider EcoStruxure software platform very nicely and links in with all of our other connected devices, including our environmental monitoring equipment through Netbots, as well as our three-phase PDUs, everything that's got Ethernet connectivity, effectively. So, yes, the UPS solutions are absolutely great for providing that emergency backup to protect critical infrastructure because, as we know, if that goes down, then all of a sudden you've got a whole site that pretty much goes offline until somebody can go and rectify the situation.

DW: *Finally, Schneider Electric is as a world leader when it comes to promoting energy efficiency and sustainability – it's pretty much in your DNA. But there are certain political developments suggesting that climate change may no longer be a major priority for business. Does that have any impact on your business? Do you dumb down your commitments as others might be perceived as doing, or are you still very much committed to sustainability and continuing lead the way?*

DM: Sustainability is still our number one priority. In the Corporate Knights rankings, we were rated the number one most sustainable company in the world for the second time, which is an absolutely fantastic achievement for us.

And we've actually redeveloped one of our programmes that was originally called Green Premium, where we have very high transparency on all of the materials, the raw materials that go into our products and talk about the energy consumption through the life cycle of a products. That's now evolved into something that we're now calling Environmental Data. If you go on to our website, we have the CO_2 carbon footprint throughout the whole lifecycle for every single product to actually allow our customers to make an informed decision on what products they want to put in and decide for themselves whether they want to also be equally as sustainable as us.

MSP CHANNEL INSIGHTS

ROADSHOW 3

Utrecht, The Netherlands

Venue: Crowne Plaza Utrecht Central Station

6 November 2025

Utrecht is rapidly emerging as a key technology hub in the Netherlands, celebrated for its innovative spirit, robust digital infrastructure, and thriving startup ecosystem.

Positioned in the heart of the country, this dynamic city is becoming a focal point for managed service providers, cybersecurity experts, and IT innovators alike.

HEADLINE SPONSOR

Kaseya®

msp-roadshow.com

Gartner reveals the top data and analytics predictions

Gartner, Inc. has announced the top data and analytics (D&A) predictions for 2025 and beyond. Among the top predictions, half of business decisions will be augmented or automated by AI agents; executive AI literacy will drive higher financial performance; and critical failures in managing synthetic data will risk AI governance, model accuracy and compliance.

DURING the recent Gartner Data & Analytics Summit in Sydney, Carlie Idoine, VP Analyst at Gartner, said, “Nearly everything today – from the way we work to how we make decisions – is directly or indirectly influenced by AI. But it doesn’t deliver value on its own – AI needs to be tightly aligned with data, analytics and governance to enable intelligent, adaptive decisions and actions across the organization.” Gartner recommends organizations use the following strategic assumptions to inform their planning over the next 2-3 years.

By 2027, 50% of business decisions will be augmented or automated by AI agents for decision intelligence. Decision intelligence combines data, analytics and AI to create decision flows that support and automate complex judgements. AI agents enhance this process by handling the complexity, analysis and retrieval of various data sources. Gartner recommends D&A leaders work with business stakeholders to identify and prioritize decisions critical to the success of the organization, and those that can benefit from more effective application of analytics and AI.

“AI agents for decision intelligence aren’t a panacea, nor are they infallible,” said Idoine. “They must be used collectively with effective governance and risk management. Human decisions still require proper knowledge, as well as data and AI literacy.”

By 2027, organizations that emphasize AI literacy for executives will achieve 20% higher financial performance compared with those that do not. Unlocking AI’s full business potential requires building executive AI literacy. They must be educated on AI opportunities, risks and costs to make effective, future-ready decisions on AI investments that accelerate organizational outcomes. Gartner recommends D&A leaders introduce experiential upskilling programs for executives, such as developing domain-specific prototypes to make AI tangible. This will lead to greater and more appropriate investment in AI capabilities.

By 2027, 60% of data and analytics leaders will face critical failures in managing synthetic data, risking AI governance, model accuracy, and compliance.

Using synthetic data to train AI models is now a critical strategy for enhancing privacy and generating diverse datasets. However, complexities arise from the need to ensure synthetic data accurately represents real-world scenarios, scales effectively to meet growing data demand and integrates seamlessly with existing data pipelines and systems.

“To manage these risks, organizations need effective metadata management,” said Idoine. “Metadata provides the context, lineage and governance needed to track, verify and manage synthetic data responsibly, which is essential to maintaining AI accuracy and meeting compliance standards.”
By 2028, 30% of GenAI pilots that move forward into large scale production will be built versus deployed using packaged applications to lower cost and increase control.

Building GenAI models in-house offers flexibility, control and long-term value that many packaged tools cannot match. As internal capabilities grow, Gartner recommends organizations adopt a clear framework for build versus buy decisions. It must factor in cost, time to market, available skillsets, integration capabilities, compliance and risk.

By 2027, organizations that prioritize semantics in AI-ready data will increase their GenAI model accuracy by up to 80% and reduce costs by up to 60%. Poor semantics in GenAI lead to greater hallucinations, more tokens required and higher costs. Organizations that rethink data management to focus on active metadata drive greater model accuracy and efficiency, have higher AI data readiness and reduce compute costs. According to Gartner, this enables AI agents to operate more effectively and facilitates smarter, faster decision making across the organization.

By 2029, 10% of global boards will use AI guidance to challenge executive decisions that are material to their business. As AI becomes embedded in board-level strategy, the need for strong data governance, regulatory clarity and reputation management will intensify. Gartner recommends boards define the boundaries of AI involvement in decision making and establish clear policies around oversight, responsibility and regulatory compliance. This will enable them to use AI as a strategic advisor while maintaining trust and control.

MANAGED SERVICES SUMMIT NORDICS

21.10.2025

STOCKHOLM WATERFRONT CONGRESS CENTER

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

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

INDUSTRY INSIGHTS

Gain actionable knowledge from expert-led presentations focused on emerging technologies, market shifts, and the evolving role of MSPs in today's digital-first landscape. Understand what's next for cybersecurity, cloud strategy, and customer success.

NETWORKING OPPORTUNITIES

Forge meaningful connections with fellow MSPs, technology vendors, and channel leaders. The summit's structure encourages open dialogue, peer learning, and opportunities to form long-term business relationships.

INTERACTIVE EXPERIENCES

Participate in demos, discover real-world case studies, and interactive panels designed to turn insights into action. These sessions let you explore solutions up close and ask the questions that matter most to your business.

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

ITEUROPA

Stephen Osborne stephen.osborne@iteuropa.com
+44 (0)7516 502689
Arjan Drayton-Chana arjan.dc@iteuropa.com
+44 (0)7516 501193

https://nordics.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS ITEUROPA ANGEL EVENTS

From dashboards to decisions -

Why artificial intelligence is the next Business Intelligence revolution

Cast your mind back to the early 2000s. Business Intelligence (BI) was having its time in the spotlight as every team wanted data at their fingertips.

BY KASIA BOROWSKA, MD AND CO-FOUNDER OF BRAINPOOL AI

BI ADOPTION skyrocketed as data hungry teams fought to utilise and make sense of siloed data - that is before IT teams stepped in to bring order to the chaos by centralising these tools and standardising processes to allow businesses to unlock value at scale.

Sound familiar? Fast-forward to today and we can see Artificial Intelligence (AI) following a similar path. But this time, the potential to transform businesses is even greater. AI is not just another new tool - it's the natural evolution of BI which allows businesses to turn data into smart decisions.

Unlike BI, AI does not require human interpretation and it can analyse and predict on its own. But, just like we saw with BI, success with AI is not guaranteed.

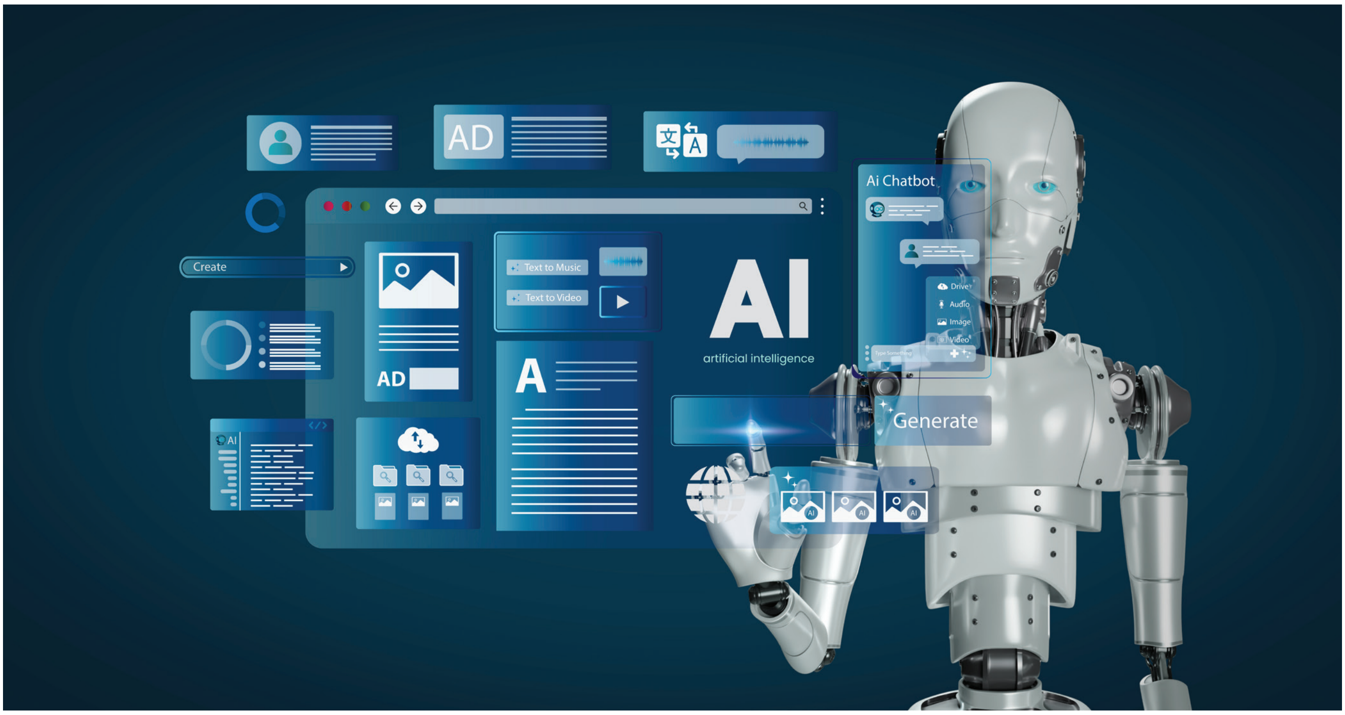
While BI helped businesses to understand what happened, AI takes this one step further by telling businesses what to do next.

But AI is only effective when used in the right way. This starts with knowing what AI should do for your business, which outcomes matter, and preparing your data accordingly.

Understanding what AI should do for your business

Unsuccessful AI implementation stems from businesses jumping straight in before considering what it should do for your business. It's easy to get distracted by the noise and implement AI for the sake of it, but real value can only be unlocked when you align AI's capabilities with your wider business needs. And this should not be rushed.

Businesses must take a step back and take the time to fully understand where the pain points, opportunities and inefficiencies are within the organisation



to identify the areas where AI can truly make a difference. This process should not be limited to one team or division - this activity should be business-wide to ensure a difference is felt across the organisation. So before you rush in, take a step back and remember that AI isn't a silver bullet - it's a strategic tool which depends on how and why it's being used. Start with the problem rather than the technology to build AI that delivers real impact.

> A good starting point for businesses is to understand what data you have, where it comes from and its intended use. To help businesses understand what data they have, they must enforce a dedicated data lineage and data change function

Priming your data to ensure success

Once you have identified the opportunities within your business, the next step is to make sure your data is ready to solve them. And this is where many businesses struggle with 78% of businesses stating data readiness is the biggest barrier to unlocking value from AI.

This statistic isn't surprising - AI is only as good as the data you feed it and if the data is unstructured, even the most advanced models will struggle to deliver what a business needs. Most businesses are sitting on a mess of data scattered across siloes - and if your input is a mess, your output will be too.

A good starting point for businesses is to understand what data you have, where it comes from and its intended use. To help businesses understand what data they have, they must enforce a dedicated data lineage and data change function. This involves tracking data through its entire lifecycle, and by creating a clear trail of this information, businesses can understand the data's source and monitor any changes to ensure its Machine Learning (ML) model runs as smoothly and efficiently as possible. Businesses should also leverage semantic modelling to improve the quality of their data. This process involves representing data in a way that accurately captures its source, which in turn allows you to understand its significance and intended use. This will give businesses a clearer picture of their data and allow them to use and process it efficiently which will strengthen their ML models.

These functions will provide businesses with a stronger and more reliable foundation for AI implementation.

Designing for outcomes, not just outputs

The true power of AI lies in its ability to deliver outcomes that are tailored to your unique business needs. Just as traditional BI tools had to be customised to fit each organisation's data strategy, AI must also be shaped around your business.

Many organisations implement off-the-shelf AI solutions in a rush to capitalise on the AI hype, but this rarely results in the desired outcomes. This is where an agnostic approach to AI becomes crucial.

By taking an agnostic approach to AI, businesses will not be tied to one specific model, platform, or provider. They will be free to plug and play different models based on what delivers the best results for each specific use case. This enables businesses to deliver more tailored and effective solutions as they will be using the best tool for each job. And this flexibility is what turns AI into the new BI.

The next generation of BI is here, but it won't succeed unless it is implemented with purpose, fueled by clean data and moulded around business' unique use cases. By focusing on outcomes, adopting an agnostic approach to AI and building strong data foundations - businesses will lead the way into our AI-enabled future. Just like with BI, the businesses who adopt AI successfully won't be the ones that adopt it the fastest, but those who adopt it the most strategically.

Making network security manageable again

Security leaders today are navigating familiar priorities under increasingly unfamiliar conditions. The objectives haven't changed: improve visibility, streamline policy enforcement, reduce misconfigurations, and maintain compliance in line with a fast-moving regulatory landscape. But delivering on those objectives has become significantly more complex – and more critical – as enterprises lean further into hybrid and multicloud architectures.

BY DAVID BROWN, SVP INTERNATIONAL BUSINESS, FIREMON

THE STRATEGIES are well understood. Zero trust, automation, and access governance are all essential components of modern security design. The frameworks are in place. The technology is available. And yet, many organisations remain stuck in a reactive posture – patching gaps, repeating manual work, and struggling to maintain policy discipline at the pace business demands.

This disconnect isn't due to a lack of awareness. It's a structural issue. As networks expand and environments diversify, policy management becomes increasingly fragmented. That fragmentation introduces risk. What's needed is a way to bring structure back into the process. This is where Network Security Policy Management (NSPM) adds real value.

From Principle to practice

NSPM isn't a standalone tool or tactical fix. It's a structured methodology that introduces clarity, consistency, and control to the way network security policies are designed, applied, and enforced. Its value lies in turning good intentions – like automation, visibility, and compliance – into practical, repeatable outcomes.

By centralising control and standardising policy workflows, NSPM helps teams move from firefighting mode to sustainable operations. It doesn't remove complexity, but it makes it manageable.

At its core, NSPM addresses three critical functions: visibility, automation, and proactive risk mitigation.

Visibility with context

The visibility NSPM enables is not simply about having data – it's about understanding the policy landscape in full. That means seeing how rules interact, where they overlap, and where there may be gaps across cloud platforms, on-prem infrastructure, and virtual environments.

Without this kind of contextual view, policy management becomes reactive. Teams can't easily see when legacy rules are still active or when changes have quietly eroded compliance. With NSPM, policies become observable

and understandable, supporting faster, smarter decision-making.

Automation with assurance

Manual policy management may have been sufficient in the past, but it doesn't scale. Firewall changes, user access updates, segmentation adjustments – these are frequent, high-stakes tasks. Relying on human intervention opens the door to delays and errors.

NSPM introduces automation into this process, but with clear governance. Policy changes follow defined workflows and templates, preserving consistency and transparency. Automation doesn't remove oversight but reinforces it.

Anticipating risk

NSPM also shifts the focus from remediation to prevention. Misconfigurations often go unnoticed until something breaks or a compliance audit brings them to light. By that point, the damage is already done.

With NSPM, policy violations, access issues, and configuration gaps can be flagged early. This not only reduces security risks but also lessens the operational burden of responding to incidents or preparing audit materials after the fact.

A Response to rising complexity

Today's enterprise networks are inherently complex. Most organisations operate across a combination of legacy systems, cloud services, and a growing edge of remote endpoints. Each environment introduces its own policies and control mechanisms, making consistency harder to enforce.

Regulatory frameworks such as GDPR, HIPAA, and PCI DSS only increase the pressure. It's not enough to simply have policies in place – they must be applied uniformly and documented in detail. NSPM makes this achievable. It simplifies compliance by embedding audit-ready processes into daily operations, rather than leaving it as a scramble at the end of each cycle.

Firewall management is a clear example. In large enterprises, change requests can number in the hundreds each month. Each needs to be reviewed, approved, implemented, and recorded. When handled manually, errors are inevitable. Gartner estimates that nearly all firewall breaches stem from misconfigurations rather than flaws in the underlying technology. NSPM is designed to reduce those risks systematically.

Operational change, not just technical integration

Adopting NSPM requires more than plugging in a new tool. It demands operational alignment across teams, especially where multiple groups manage different parts of the network. Integrations must be mapped across existing systems, and policy workflows may need rethinking. There's also a cultural shift involved. In many teams, policy management has long relied on individual expertise and direct control. Moving to structured, automated enforcement can feel unfamiliar. But NSPM doesn't diminish that expertise, it gives it a framework to operate more effectively.

Starting with a phased rollout and focusing on low-risk policy areas can help ease the transition. What matters is that NSPM becomes a living part of the security lifecycle: enabling regular policy reviews, improving coordination, and ensuring that insight leads to action.

Security that scales

Perhaps NSPM's greatest strength is its adaptability. It isn't bound to a particular platform or vendor. Its principles – centralisation, standardisation, consistency – can be applied across architectures and industries. That makes it valuable not only now, but as infrastructure continues to evolve.

As security teams face rising expectations and expanding attack surfaces, process discipline becomes as important as technical capability. NSPM offers a way to scale that discipline without increasing operational strain.

It turns best practices into working practices. And it helps organisations maintain clarity, control, and resilience – no matter how fast the environment moves.

> By centralising control and standardising policy workflows, NSPM helps teams move from firefighting mode to sustainable operations. It doesn't remove complexity, but it makes it manageable

AI and analytics are built on strong data foundations

The rapid adoption of AI shows no sign of slowing down as more businesses look to develop AI products and services to drive growth and innovation. But delivering data to AI models is not easy, and many will soon discover their data infrastructure may not be adequate to support them on their AI journey.

BY JUSTIN BORGMAN, CEO, STARBURST

AI IS ONLY as good as the data that it can access and learn from. Which is why enterprise data stacks need to evolve to become AI data stacks capable of supporting the next generation of AI applications. Fortunately, the fundamentals are already in place. Businesses can leverage the data architecture and solutions that were built for data analytics to power AI workflows and feed their AI and ML models.

The truth is that analytics and AI are just two halves of the same data problem. They both turn raw data into insights that solve real business problems, and both rely on strong foundations built using data architecture.

However, data never stands still, and today there are new frontiers of value, particularly in relation to AI.

It is because of this that businesses are developing a new foundational layer for an AI data architecture to power new applications and services, as well as the underlying infrastructure that supports them.

What can AI do for you?

AI is only as good as the data it can reach, but enterprise data is fragmented, siloed and often outdated. To capitalise on their AI investments, businesses need an AI data architecture that spans their cloud and on-premises environments, accelerates AI innovation, and solves business problems faster.

To achieve this, AI needs a scalable data architecture that accesses data from multiple sources in multiple formats while governing it securely.

That's why businesses are adopting solutions that use the same data lakehouse architecture used for data analytics to feed their generative AI and machine learning (ML) models. These technologies are capable of serving AI workloads to remove bottlenecks in AI data workflows, exactly like it helped to remove them for data analytics. Years of development and evolution have led to the convergence between the needs of data analytics and AI. To the extent that today, answering the question, "What can your data do for you?" increasingly means going beyond analytics, it's referring to AI.

Optmising the AI data stack

There is no AI without data. Not a single AI model operates without data to train on, and the continued flow of data into models allows them to grow. In this sense, data is the foundation, not just the foundation of analytics but also the foundation of AI. What you build on top of it depends on your ability to build that foundation in a secure, reliable, and predictable way.

Essentially, the platform you used to power your analytics data stack can also be optimised to power your AI or ML data stack. It could power the data stack that drives your business intelligence dashboards, your data applications, or your AI models, acting as both an SQL query engine and an AI query engine. The same things that make an analytics data stack successful also make an AI data stack successful. In both cases, data needs to be accessible, organised, and governed. With AI growing so fast, there is a huge and growing demand to build data foundations in every business, whether they use AI today or are thinking of adopting it tomorrow.

Laying the foundation for AI data

Regardless, businesses need to overcome the inherent challenge of accessing fragmented and siloed data. The fact is that data silos in AI are no different from data silos in data analytics, and they hold back the ability to derive value from your data. The solution lies in adopting a platform that provides you with a single foundation for all your AI data, one that provides you with a strong data stack capable of supporting your AI models.

That platform needs to be built to scale data governance as quickly as it scales data itself. This is already a focus for data analytics, where it creates a secure foundation for your data across multiple environments–cloud, on-premises, and hybrid–ensuring that the right people can access it in the right way. It also needs to be easy to use. This means that as your team works to pull together data sources, identify context, and feed this into an AI model, their energy and efforts create results. Essentially, speeding up your ability to move from development to deployment, to go from AI proof of concept to full-scale productive intelligence. This process will power the foundation of your AI architecture to help you get the most value from your data, whether that means analytics or AI.

Connecting the dots between AI and analytics

Data architecture has always had a huge impact on the success of data analytics, which is exactly why getting this technology right has meant the difference between success and failure throughout the history of big data. With the shift towards AI, data architecture is once again in focus.

Just like before, a good foundation for this data architecture is essential. Without data, you don't have anything. That's true of data analytics, and it's also true of AI. And while AI expands the possibility of business value in new and exciting ways, achieving those objectives remains rooted in business value. That's why it's essential to have a platform that provides the foundation for all your data, encompassing analytics and AI.

Five steps enterprise can take to prepare for Agentic AI

The shift and maturation of agentic AI won't happen overnight. Take concrete steps now to help position your business to fully leverage the transformative power of this technology.

BY MICHAEL NAPPI, CHIEF PRODUCT OFFICER, SCIENCELOGIC

AGENTIC AI is rapidly evolving to shape the future of technology and technology management as we know it. While its widespread adoption is still on the horizon, momentum is building. Gartner calls agentic IT "one of the hottest topics and perhaps one of the most hyped topics in gen AI today," and forward-looking enterprises are already investigating what it will take to tap into its potential to drive efficiency and deliver a competitive edge.

At its core, agentic AI refers to AI systems that can independently make decisions, initiate actions, and execute tasks without continuous human oversight. In today's complex and fast-moving IT environments, agentic AI promises to revolutionize operations by enabling systems to operate autonomously, optimize performance, and improve operational agility.

This leap forward has significant implications:

- **For IT leaders,** it improves system health and resiliency, promotes self-healing and self-optimized environments, shortens ramp-up time for new employees, and frees teams to focus on more strategic initiatives.
- **For business leaders,** it increases productivity, reduces costs, reduces time to market for new innovations, and enhances customer experiences.

But to ensure success, agentic AI requires a foundational readiness that many organizations have yet to build. From observability to data readiness to "learning to let go," and more, here are five steps your organization can take to prepare for agentic AI.

Modernize IT operations

The good news is that most organizations are already taking the first step: modernizing their IT operations. This means consolidating fragmented tools and technologies to create a unified, real-time view of the IT estate – a single source of truth.

This is foundational to agentic AI because agents can't make smart decisions or take meaningful actions without a complete picture of what is happening. You can't manage, or automate, what you can't see. So, discovery and observability are key. They provide agentic systems with the critical insights they need to understand the environment, identify issues early, and act on them proactively.

Focus on data readiness

Data integrity and accuracy – both key to achieving a single source of truth – are surprisingly unsolved problems in IT. For example, many IT organizations lack discovery tools, and manual updates to CMDBs are common, which can severely impact data accuracy.

Agentic AI relies heavily on observability and an accurate map of the IT environment. If the CMDB is wrong, the agent's understanding of the environment becomes flawed, potentially leading to incorrect assumptions or unintended, risky actions that could jeopardize operations.

The goal is to have a comprehensive, real-time view of your infrastructure. Not a static snapshot that gets refreshed every two weeks.

Identify automation use cases

Next, look for automation opportunities. Identify frequent, redundant, or error-prone activities. Those are your low-hanging fruit for automation. With agentic AI, you can start assigning those tasks to digital agents.

Review where your team is spending operational time. Create a backlog of those tasks and assess where automation can have the most impact. Then, consider the tools or technologies you'll use to automate them. One very basic example is password resets. It's the most common task IT service desks handle and one that most companies have already automated due to its repetitive nature.

Another example is onboarding new employees. Provisioning accounts, setting up access to business systems, issuing devices, adding them to distribution lists, etc. is a multifaceted, multistep task that touches many systems and is a great candidate for automation.

Implement governance

Agentic AI is moving fast. Some experts say that agents will outnumber humans in the next 3 years. That kind of growth creates complexity. If you have a network of semi-autonomous agents interacting with each other, you can quickly reach a point where no single person fully understands all the interactions. This non-deterministic behavior can create significant security and compliance risks.

Hence, the importance of starting with simple, well-understood use cases. Build agents that perform basic, repetitive tasks and make sure you understand how they operate. Additionally, it's essential to have management platforms in place for your agents – systems that provide an audit trail, explainability, and oversight. AI agents are just applications. They're fueled by LLMs, exposed via APIs (e.g. MCP), and assigned goals. But you need instrumentation, training, and management tools to ensure an sbility to understand and govern their execution.

Learn to let go... when you are ready

Despite agentic AI gaining traction, there is still understandable hesitation regarding autonomous AI and a lack of human control and oversight.

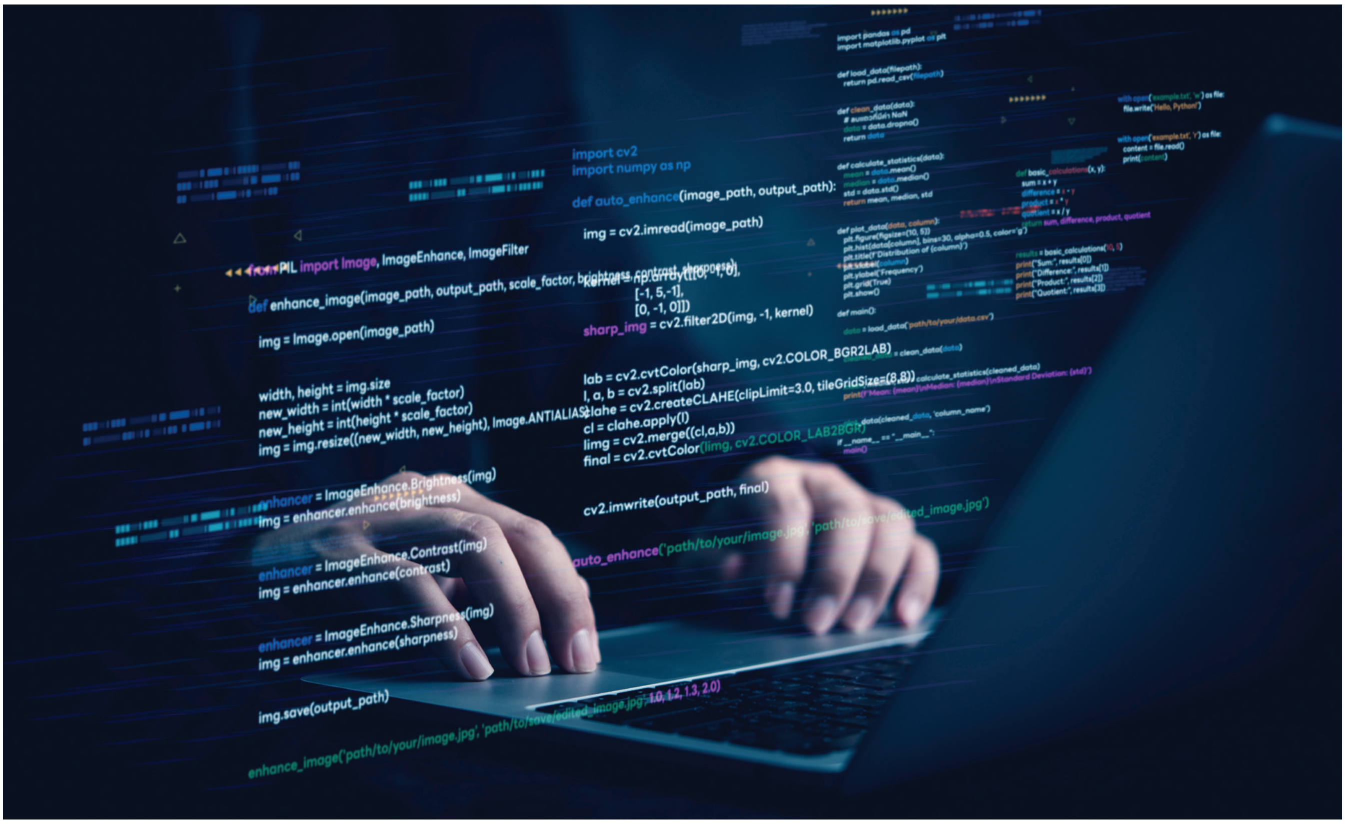
Transparency and explainability are helpful, but ultimately, your organization must determine the level of control it wants to retain, based on your industry and existing governance controls, as well as the functions you intend to automate

The key is to ensure that any agentic AI platform offers the flexibility and control your business needs. Companies should wade into Agentic AI with due deliberation, and ensure there are "humans in the middle" of critical business workflows until the company has developed enough trust and experience in Agentic-driven processes and how to manage them

Maturing your agentic AI strategy

Agentic AI is not a distant vision. It is here today. Early implementations are already emerging, and progressive enterprises are starting to pilot simple, single-agent tasks. Others have gained confidence and begun adopting agents that collaborate within a controlled ecosystem, beginning to operate across broader segments of the enterprise. These agents share real-time updates, escalate issues to humans or other agents, trigger actions (such as security updates), and monitor compliance with policies and regulations.

But the shift and maturation of agentic AI won't happen overnight. Take concrete steps now to help position your business to fully leverage the transformative power of this technology.


import cv2
import numpy as np
def auto_enhance(image_path, output_path):
img = cv2.imread(image_path)
from PIL import Image, ImageEnhance, ImageFilter
def enhance_image(image_path, output_path, scale_factor, brightness, contrast, sharpness):
img = Image.open(image_path)
width, height = img.size
new_width = int(width * scale_factor)
new_height = int(height * scale_factor)
img = img.resize((new_width, new_height), Image.ANTIALIAS)
sharp_img = cv2.filter2D(img, -1, kernel)
lab = cv2.cvtColor(sharp_img, cv2.COLOR_BGR2LAB)
l, a, b = cv2.split(lab)
clahe = cv2.createCLAHE(clipLimit=3.0, tileGridSize=(8,8))
cl = clahe.apply(l)
limg = cv2.merge((cl,a,b))
final = cv2.cvtColor(limg, cv2.COLOR_LAB2BGR)
cv2.imwrite(output_path, final)
img.save(output_path)

How safe is the code you don't write? The risks of third-party software

Third-party code is a double-edged sword. On the one hand, it's indispensable. On the other hand, it's a potential liability.

BY NEIL ROSEMAN, CEO OF INVICTI SECURITY

IT'S NO exaggeration to say that modern software runs on open source. Every product, platform, and digital experience we rely on, whether built by scrappy startups or global enterprises, leans heavily on third-party components.

This is no accident. Open-source and commercial packages and public libraries accelerate innovation, drive down development costs, and have become the invisible scaffolding of the Internet. GitHub recently highlighted that 99% of all software projects use third-party components.

But with great reuse comes great risk.

Third-party code is a double-edged sword. On the one hand, it's indispensable. On the other hand, it's a potential liability. In our race to deliver software faster, we've created sprawling software supply chains with thousands of dependencies, many of which receive little scrutiny after the initial deployment. These dependencies often pull in other dependencies, each one potentially introducing outdated, vulnerable, or even malicious code into environments that power business-critical operations.

The result? A software ecosystem where trust is assumed but rarely verified.

When trust becomes a threat

Even the most sophisticated software organizations can be caught off guard. A relatively recent example comes from a long-standing open-source project: polyfill.io, a widely used library that helps ensure JavaScript compatibility across browsers. For years, it was seen as a safe and helpful tool to smooth out any differences in cross-browser support. But one day, the domain along with the CDN distributing the library was quietly sold and repurposed by a new maintainer—who began injecting malicious payloads into the polyfills being served to millions of users.

This wasn't a zero-day exploit or a novel vulnerability. It was a supply-chain hijack hiding in plain sight. And it worked because we tend to treat third-party code as static and safe. Once integrated, it often becomes invisible. Similar incidents are becoming the rule, not the exception. I saw an ESG report last year that found a staggering 91% of surveyed organizations experienced some form of software supply chain attack in the preceding 12 months.

That's a big number. Increasingly, attackers aren't bothering to storm the front gate anymore—they can simply walk in through a side door marked "npm install."

First-party diligence, third-party blind spots

Many development teams have processes in place for reviewing first-party code. We have code reviews, security testing, and CI/CD pipeline checks, all designed to catch issues before they make it to production.

And yet that same rigor rarely applies to third-party packages. Why? Because we don't own them. Because they're "someone else's responsibility." Because updating or removing them feels too risky, too disruptive, or too complex.

Ironically, even though these dependencies often make up the majority of an application's actual codebase, many remain completely unmonitored after initial vetting, adoption, and deployment. This lack of visibility creates fertile ground for attackers and leaves organizations scrambling to react when something goes wrong.

The latest AI code generation tools make this situation even worse. There is solid evidence that while we believe AI-generated code is more secure than our own, it is actually less so. Combine that with it being in a third-party component and you have a recipe for vulnerability.

It's not just what's in your code – it's what your code trusts

When we think about software risk, we tend to focus on newly created code. It's the most visible and also the most important part of the application. It's where the business logic and business value reside. From a security standpoint, though, all those meticulously checked new bits are only one small part of the overall attack surface.

A more accurate threat model needs to go far beyond first-party code to encompass everything your applications are running, whether or not you deliberately put it there. This includes transitive dependencies where a single package pulls in dozens of dependencies—many of which will be unknown to the developer.

Hiding in that crowd could be abandoned libraries that quietly do their job but haven't been actively maintained in years, bringing any of their existing or newly discovered vulnerabilities into your environment. And that's before you even get to the threat of deliberate malicious action to compromise or impersonate popular packages or their distribution networks, as with Polyfill.

Any of these scenarios can lead to real-world consequences. From data exfiltration and credential theft to full-scale breaches, third-party compromises have become a preferred tactic for adversaries—because they're often easier and more discreet than breaking down the front door.

Rethinking what we trust

The risk is real, so what do we do? We can start by treating third-party code with the same caution and scrutiny we apply to everything else that enters the production pipeline. This includes maintaining a living inventory of all third-party components (including transitive dependencies) across every application and monitoring their status to prescreen updates and catch suspicious changes.

With so many ways for threats to hide, we can't take anything on trust, so next comes actively checking for outdated or vulnerable components as well as new vulnerabilities introduced by third-party code. To cover all bases and catch all dependencies, start with conventional static code and component checks but be sure to also run dynamic tests in development and after deployment. Static scans alone won't tell you if something deployed last year has become dangerous today.

> A more accurate threat model needs to go far beyond first-party code to encompass everything your applications are running, whether or not you deliberately put it there

Finally, build component distrust into your operational security model (which you should be doing anyway). Establish strong update policies that don't leave libraries to age unchecked for months or years on end. Define SLAs for security patches and involve security teams early when considering new packages.

Ultimately, we all need to adopt a zero-trust mindset toward third-party code. That doesn't mean blocking its use – but it does mean validating continuously, assuming risk, and building processes that can catch drift before it becomes a disaster.

Trust but verify – and keep verifying

In software, we've come to view dependencies as safe because they're so helpful and so common. But ubiquity isn't the same as security.
The reality is that third-party code behaves like any other code: it evolves, it changes, and it can be compromised. The only difference compared to your in-house repos is who controls it—and in most cases, that's not you.

Speaking as the CEO of a cybersecurity company, I believe it's time for all of us in the tech industry to confront the (possibly uncomfortable) truth: third-party code is an inevitable and massive part of our attack surface. If we don't treat it that way, we're gambling with our customers' trust and the integrity of our businesses. At Invicti, we believe that starting with frequent scanning using our DAST-first approach is the best way to secure your application environment from the outside in.

The way forward isn't to ban third-party code or build everything from scratch. That's neither practical nor scalable. The answer lies in awareness, oversight, and tooling that gives you real visibility into what your applications rely on—and how those dependencies behave, not just when first deployed and tested but every day thereafter. Because whether or not you are watching your software supply chain, potential attackers are.

Why embracing an AI-powered multi-cloud approach is now critical

By deploying an AI-driven cloud management platform, organisations can reduce the complexities of managing multi-cloud environments and streamline operations across different cloud providers and environments.

BY DIRK ALSHUTH, CLOUD EVANGELIST AT EMMA – THE CLOUD MANAGEMENT PLATFORM

THE GLOBAL MARKET for Artificial Intelligence (AI) infrastructure is set for significant growth, with the International Data Corporation (IDC) projecting AI infrastructure spending will surpass $200 billion by 2028. During the first half of 2024, organisations boosted their investment in compute and storage infrastructure for AI deployments by 97% compared to the previous year, totalling $47.4 billion.

As a result, it is now critical for organisations to reevaluate their current infrastructure to support these increasingly resource-intensive workloads. Businesses must address not only the immediate requirements but also plan for scalability and viability, ensuring that their systems can continue to meet the evolving demands of AI technologies in a highly competitive market.

The emergence of new AI workloads is reshaping requirements for cloud infrastructure, demanding scalable storage and low latency environments to achieve optimal performance. They also demand heightened oversight due to new regulations like the EU AI Act, which enforces strict transparency, risk management, and compliance standards. This introduces further complexity for businesses dependent on cloud services.

For businesses navigating these evolving demands, flexibility stands out as an essential requirement. In the past, businesses have trusted hyperscalers like AWS and Azure to dominate the cloud scene, but relying entirely on one or more hyperscalers, or only one cloud environment is becoming unsustainable. Therefore, organisations must consider deploying a future-proof cloud strategy that allows them to tap into the strengths of different providers and environments, ensuring better operational continuity while adhering to regulatory requirements and optimising costs.

Leveraging multi-cloud for AI workloads

Multi-cloud strategies offer superior flexibility and resource diversity compared to single-cloud or hybrid options. They allow businesses

to strategically spread workloads across various cloud environments to effectively manage resource scarcity, stabilise uptime and performance, optimise costs and ensure compliance with shifting regulations.

By selecting infrastructure specifically suited for their workloads, businesses can access AI services from multiple providers, but are also faced with increased complexity to manage their cloud operations expanding from conventional to AI-optimised resources.

While the benefits of multi-cloud environments are clear, they also come with several challenges – complexity, cloud sprawl, cost and data security and compliance. Organisations must address these to maximise their benefits. Finally, the lack of centralised tools to efficiently manage multi-cloud operations often leads to inefficiencies. This complexity is compounded by the scarcity of skilled professionals equipped with the specialised knowledge required to navigate these ecosystems, further amplifying operational hurdles.

While the benefits of multi-cloud adoption are significant, organisations must address these challenges head-on to fully realise its potential.

Why a smart multi-cloud strategy needs AI-powered intelligence

Managing the complexity of multi-cloud environments without AI-powered capabilities is like flying a plane without instruments.

Limited visibility often leads to inefficient resource use, higher costs, and underutilised infrastructure. Without AI-driven insights, identifying performance issues or predicting downtime becomes harder, increasing the risk of service disruptions and eroding customer trust.

Additionally, staying compliant with ever-changing regulations becomes more difficult without proactive monitoring, leaving organisations vulnerable to fines and legal risks. Leveraging AI-powered solutions isn't just a nice-to-have, it's essential for boosting operational efficiency, staying competitive, and ensuring your multi-cloud strategy is smart, scalable, and future-ready.

Here's how this can be achieved:

- **Greater agility and flexibility**
  Adopting an AI-enabled multi-cloud strategy significantly enhances organisational agility and flexibility. As businesses increasingly face dynamic market conditions, leveraging AI-driven insights enables organisations to gain foresight for proactive resource management, anticipating demand and strategically allocating resources to align with business goals. Intelligent automation takes care of routine tasks and accelerates the deployment of applications and services, providing the flexibility needed to adapt to changing business demands and to remain competitive.
- **Enhanced cost management and budgeting**
  Managing costs is crucial in a multi-cloud setting, yet traditional tools often rely on manually reviewing past spending patterns rather than predictive analytics. Such limitations confine organisations to reactive strategies due to imprecise cost forecasting. AI-driven cost management capabilities provide real-time visibility across diverse cloud environments and comprehensive insights to allow organisations to act on recommendations.

  By accurately forecasting future cloud expenses through the analysis of current and past usage trends, organisations can make proactive decisions and ensure financial accountability. Advanced features like automated cost optimisation, intelligent resource rightsizing, and scenario modelling enable precise workload placement and provide comprehensive insights, achieving significant cost savings while maximising business value.
- **Heightened security and resilience**
  AI-driven security management strengthens resilience by proactively identifying and responding to potential threats. Predictive analytics capabilities analyse vast amounts of data, quickly detect anomalies and mitigate risks through automated threat detection and response, without the need for human intervention. This provides rapid protection against evolving threats. By forecasting potential incidents, predictive analytics enable proactive security measures and optimal resource allocation. Continuous monitoring of cloud environments allows them to identify vulnerabilities before they escalate, ensuring swift response and risk mitigation. This helps businesses maintain continuity during potential disruptions, protective operations and data integrity.
- **Efficient workload optimisation**
  Organisations can benefit from AI-powered workload optimisation capabilities by identifying the best cloud providers and environments for specific tasks, enhancing performance and efficiency. By assigning workloads to the most appropriate environments, organisations can fully harness the full potential of their traditional and AI workloads. This includes cost optimising through dynamic resource allocation and achieving scalability without manual intervention.

Transforming cloud infrastructure with AI integration

AI is fundamentally reshaping the landscape of cloud infrastructure. Both with regards to different types of resources and how these are managed. With the growth of AI adoption, organisations need to strategically spread workloads across various cloud environments to effectively manage resource scarcity, optimise costs and stabilise performance. Multi-cloud strategies offer superior flexibility and resource diversity compared to single-cloud or hybrid options.

By deploying an AI-driven cloud management platform, organisations can reduce the complexities of managing multi-cloud environments and streamline operations across different cloud providers and environments. Leveraging AI for data analytics allows businesses to derive deeper insights from multi-cloud data sources, facilitating informed decision-making. This enhances their operations, creating an environment prepared for continuous innovation.

By embracing this strategy, businesses not only meet market needs and regulatory requirements but also gain a competitive edge. They can unlock new opportunities for growth, improve overall efficiency and drive innovation, themselves for long-term success.

Safeguarding connected industries with smarter cloud deployments

According to Statista figures, the number of IoT devices around the world will reach 32.1 billion in 2030, more than double the 15.9 billion reported in 2023. As this technology expands in use, connected systems offer promise by transforming industries such as manufacturing and transportation with expanded efficiency, valuable real-time insights and automated processes.

BY JAMES PENNEY, CTO, DEVICE AUTHORITY

If we look at the manufacturing sector, sensors can continuously monitor machinery performance, allowing for predictive maintenance and reducing the risk of expensive failures. In transport, IoT devices deliver real-time data on vehicle performance, driver behaviour and traffic conditions, enabling improved fleet management and road safety.

As the manufacturing and mobility sectors become more dependent on these devices, it's ever more crucial to safeguard them against evolving cyber threats, while ensuring their operational efficiency isn't hindered in any way. But many organisations now use advanced digital architectures to connect operational technology, industrial systems and IT environments, adding complexity to the process of securing every endpoint in the network. A single compromised device can lead to data breaches, production disruptions or safety risks.

The rise of Industry 4.0 reinforces the need for built-in protections that safeguard users and systems without disrupting daily operations.

Machine identity management and automation

Reinforcing IoT security is a multi-faceted task, and automating identity management can help by reducing the burden on human resources. When factories and supply chains become more connected, the number of machine identities - ranging from cameras and sensors to autonomous vehicles - often surpasses human identities by a wide margin.

This type of scale is hugely difficult for staff to manage, leading to discrepancies in device authentication and credential updates. Automated workflows for identity and certificate management help solve this challenge. For instance, digital certificates can be generated, assigned, and periodically renewed through predefined policies, ensuring that devices always have current credentials. Automation also covers password rotation and immediate credential revocation for decommissioned devices, which prevents overlooked accounts from becoming weak links in the system.

With process standardisation at play, manufacturers can navigate the challenge posed by staff leaving the business or the rapid introduction of new devices. This approach both heightens security and frees up IT teams to concentrate on higher-level objectives rather than repetitive manual tasks.

Real-time threat monitoring

Visibility of every connected device is also crucial to achieving best-practice IoT security. Continuous monitoring allows organisations to detect unauthorised activities or system anomalies before they escalate.

Instant alerts can detect unusual surges in data traffic, unauthorised attempts to access restricted network areas, or unexpected interactions between devices that should not be communicating. Swift detection means teams can isolate or disconnect compromised devices, analyse incident details, and respond before threats spread deeper into an environment.

Comprehensive logs and audit trails strengthen these efforts by recording user access, configuration changes and device activity. This makes it easier to trace suspicious activities back to their origin and to understand how hackers might exploit potential system weaknesses.

Regulations including GDPR and HIPAA demand that businesses keep detailed logs of how data is being safeguarded. Automated threat intelligence solutions that integrate with these monitoring systems further strengthen resilience by interpreting real-time data and highlighting urgent priorities for security teams.

Strengthening these defences helps manufacturers build confidence in digital transformation initiatives, which rely on strong device and network security to maintain steady productivity.

The invaluable role of the cloud in unified identity management

Integrating these measures into a unified framework is essential for achieving secure and scalable IoT. Organisations often rely on a variety of devices in different locations, which complicates credential oversight and policy enforcement.

A centralised identity management approach provides a single control point for assigning access rights, revoking access, and enforcing consistent security policies. This approach extends time-tested principles such as privileged access management, widely used in IT, to IoT and operational environments. Authorised administrators can decide precisely which devices or systems a given user can access, how long that access remains valid, and what level of authentication is required.

Cloud-services are proving popular with manufacturers when overseeing these technologies. A cloud-first model simplifies expansion and ensures consistent security management as new devices come online.

Rather than relying on fixed hardware investments and manual processes at each facility, security teams can manage large-scale IoT deployments through a single interface.

This allows for greater freedom in deploying software updates and addressing vulnerabilities across dispersed operations. It can also streamline data collection and analysis by funnelling raw insights from devices into a central repository, where advanced analytics or machine learning tools can identify trends and emerging threats.

Cloud-based designs can being numerous advantages, but the implementation process needs to be carefully considered. Compliance requirements differ across industries, so it is vital to choose a cloud partner that meets data governance mandates and provides robust encryption both in transit and at rest. Strong integration between cloud services and on-site equipment also matters, ensuring that a device's security posture is consistent whether data is processed on premises or in the cloud.

A close working relationship between operations teams and IT staff is essential for conducting a comprehensive risk assessment, pinpointing critical systems and determining the best ways to protect them.

The benefits of IoT, such as optimising production, lowering costs and enhancing service quality, are significant, but they rely on a secure foundation. Automation simplifies the management of machine identities, continuous monitoring detects suspicious activity before it spreads, and centralised identity controls close security gaps that could be exploited.

Implementing these strategies within a well-structured, cloud-driven model supports rapid scaling and compliance with evolving regulations.

As industries become more connected, strong security is both a safeguard and an enabler of long-term innovation, allowing organisations to expand their digital operations without negatively impacting on integrity.

Navigating the unexpected security issues of the agentic AI revolution

The rise of agentic AI is no longer a distant possibility, it's underway. A recent Gartner study predicts that by 2028, 33% of enterprise software applications will incorporate agentic AI, a substantial increase from the less than 1% in 2024.

BY YUVAL MOSS, VICE PRESIDENT OF SOLUTIONS FOR GLOBAL STRATEGIC PARTNERS, CYBERARK

AI AGENTS or agentic AI are systems designed to perform tasks or make decisions on behalf of users. They interpret surroundings, process information and accomplish specific objectives, continuously learning and improving through advanced algorithms and machine learning. This makes them crucial for driving productivity and improving efficiency, and an invaluable asset for businesses.

As these autonomous AI agents take on more responsibilities across businesses, their impact is set to be transformational. But with this evolution comes new and unexpected security challenges, some of which many businesses are not fully prepared for.

While AI agents are not yet widely used in the enterprise, adoption is accelerating quickly as organisations realise the huge benefits they bring.

Employees across all levels and their associated identities – from business users to IT professionals to developers, and even to the devices and applications they use – will soon start interacting with resources and services through AI-powered agents.

These agents will be embedded into operating systems, browsers and platforms, as well as everyday tools like Microsoft Teams. Companies will even start to develop their own agents or use agents-as-a-service provided by SaaS providers.

By learning to work alongside a combination of AI-driven agents, employees' productivity has the potential to skyrocket. These AI driven agents will not only streamline workflows but also redefine how tasks are delegated and executed, effectively transforming users into managers of their own virtual teams. This shift will fundamentally reshape traditional roles, making work more dynamic, efficient, and strategically focused.

So, given their ability to integrate seamlessly into business operations and simplify multiple workloads, organisations will find it impossible to avoid adopting agentic AI. The key challenge then, is understanding and mitigating the security implications.

The unseen autonomy of shadow AI agents

One of the biggest security challenges is the rise of shadow AI agents, in other words, AI-powered tools that have been deployed without the knowledge of IT and security teams. These agents can be introduced by individual employees, often bypassing standard security processes.

Because these agents can function independently and without supervision, they can introduce risks in unforeseen areas, creating blind spots for security teams. Without proper oversight, they can become a significant security vulnerability with the potential to expose sensitive company data or provide entry points for malicious actors.

Developers as the new R&D and operations experts

The role of developers is also evolving. No longer just coders, they are now key players in research, development, and operations. Generative AI has already enhanced developer productivity, but now this is going one step further.

Developers will soon manage the entire application lifecycle, from coding and integration to QA, deployment and troubleshooting – all autonomously.

With this increased autonomy comes increased privilege. If a developer's identity is compromised, the risk escalates dramatically, making it one of the most valuable, but also vulnerable identities in the enterprise.

Securing these identities must therefore be a top priority to prevent attackers from exploiting AI-powered development environments.

The risks and impacts of having humans in the loop

As organisations integrate agentic AI, humans will still continue to play a critical role in oversight and governance. These 'human-in-the-loop' process are essential for validating and ensuring that AI agents operate as intended, validating their actions, and approving exceptions and requests from agents. Human input will also shape the future behaviour of these self-learning AI agents.

However, malicious actors may target these individuals to infiltrate the architecture, escalate privileges and gain unauthorised access to systems and data. Balancing the necessity of human oversight with strong security measures will therefore be essential to minimising risk.

Managing millions of AI Agents

One of the biggest hurdles for enterprises is the sheer scale of AI agent deployment. Machine identities already outnumber human identities by up to 45-to-1, and 76% of security leaders anticipate the number of machine identities in their organisation to increase by as much as 150% over the next year.

Meanwhile, NVIDIA's Jensen Huang's predicts 50,000 humans could manage 100 million AI agents per department, meaning the ratio could soar to over 2,000-to-1.

To maintain security, best practice will involve dividing tasks among multiple specialised AI agents, each with defined roles and responsibilities to help mitigate risk and maximise efficiency.

Advancing security for agentic AI
For the successful deployment of agentic AI at scale, organisations must place a strong emphasis on safety, regulatory compliance, and building trust in their systems.

Key requirements for this include full visibility into activities, strong authentication mechanisms, least privilege access, just-in-time access controls as well as comprehensive session auditing to trace actions back to their identities. Doing this is vital for ensuring the security of both human and machine identities alongside the rise of agentic AI.

It's important to note that given the rapid pace of advancements in this field, we could not have anticipated many of the challenges discussed here just a few months ago. While not exhaustive, the examples highlighted above reveal the dramatic shifts and potential risks associated with the widespread adoption of agentic AI.

As agentic AI continues to reshape enterprise operations, organisations must stay vigilant. While new challenges continue to arise, one thing we know for sure is that it is here to stay and the question isn't whether enterprises will adopt it, but how they'll secure it.

DW ROUNDTABLE
Modern Enterprise It - From The Edge To The Core To The Cloud
Not every discussion is a **battle...**

The role of smart networks in meeting sustainability goals

It's been a long time since sustainability was a mere buzzword. These days it is a critical concern for organisations globally and there are few (if any) enterprise businesses that don't have statements professing their environmental credentials and green commitments.

BY MITTAL PAREKH, SENIOR DIRECTOR, PRODUCTS, RUCKUS NETWORKS, COMMSCOPE

ONE KEY certification many enterprises strive for is LEED (Leadership in Energy and Environmental Design), the world's most used green building rating system. It aims to help building owners and operators be environmentally responsible and use their resources efficiently.

The LEED certification is multi-faceted, and there is no one way in which an organisation can earn it. While the certification path may not be straight, what is clear is that improved sustainability begins with network efficiency.

The role of network efficiency

Smart IoT solutions, intelligent monitoring, and automation can significantly benefit business sustainability by optimising energy efficiency, water management, waste management, and procurement. By connecting company systems to the network, IoT allows them to communicate and share data. This connectivity enhances the efficiency and effectiveness of sustainability initiatives, such as those required for LEED certification, by providing real-time data and automated control over various processes.

Enterprise networks often contain a wide range of technologies, including wired Ethernet, Wi-Fi 7, Bluetooth, other IoT protocols, and private 5G. Each of these has a specific role, and there are numerous ways to combine them during implementation, depending on the industry in focus. Let's explore how these technologies are applied in the retail sector.

Retail

Retail is one of the more diverse and technologically advanced sectors. Retailers promote their sustainability credentials knowing they influence

customers' preferences as to where to shop. One widespread waste-saving initiative is retailers switching to eco-friendly packaging to minimise their environmental impact. However, the opportunities for network-based, efficiency-driven sustainability improvements go far beyond this.

An intelligent network offers retailers numerous ways to further reduce their carbon footprint. Beyond the green measures of digital receipts, electronic shelf labels, and digital signage to replace printed materials, there are greater, system-level opportunities that can strategically enhance the resource-conserving efficiency of the network. For instance, smart management of power systems makes it possible to turn off connected devices, including lighting in unoccupied areas, thereby reducing energy. That's been common for some time, what's newer is the ability to do things like rebalancing Wi-Fi coverage across a particular area, ensuring that the signal is where it needs to be to suit customer and network demands.

Additionally, AI can dynamically adjust heating and cooling systems to reduce energy usage and costs without compromising customer comfort, enabling retailers to meet their sustainability goals. This advanced capability ensures that environmental control systems are optimised for efficiency, further contributing to the overall reduction of the carbon footprint.

Introducing AI

A recent and significant change to network capabilities is the widespread adoption and rapid development of AI as a design, configuration, management, monitoring and even optimisation solution. AI is now a priority in the retail sector, as it is in every enterprise environment where the number and complexity of connected technologies are growing. Managing these layered technologies is nearly impossible for humans alone. Even with a large IT staff, it would be complex. AI allows staff to focus on other valuable tasks instead of, for example, deciding when to turn services on or off. Indeed, AI and automation can constantly review store traffic and optimise settings as needed. With experience, AI can even learn to predict traffic patterns, making the network even more efficient and reducing the need for human input to the most basic overview.

Retail industries associated with perishable goods particularly benefit from AI's proactive issue resolution capabilities as maintaining specific temperature ranges is crucial to preventing spoilage. AI can detect and resolve network issues before they impact operations, ensuring that food is stored correctly and reducing waste. AI can further assist sustainability efforts through water monitoring and management. Leaks can be rapidly identified, and water use in other operations (such as cleaning) optimised to keep costs low and waste minimal. Through modern IoT sensors and controls, AI can designate that power and water are only consumed to serve a specific purpose.

Across the retail industry, businesses face a trifecta of challenges: IT is getting leaner, margins are getting thinner, and there is a mandate to meet or beat sustainability goals. AI-driven networks provide a solution by delivering self-healing and proactive management of networks that require minimal IT involvement. This reduces the number of truck-rolls to physical retail locations to fix network issues, directly lowering the carbon footprint and IT costs. Every single truck-roll counts when margins are thin.

Supporting, not replacing, staff

In 2025, the IT industry has reached a pivotal understanding: AI is not here to replace teams, but to enhance their capabilities. AI is supporting IT professionals to work smarter and more efficiently. By automating routine tasks, it is freeing up their time, allowing them to focus on more complex and innovative aspects of their work. This boost in efficiency means they are achieving more in less time and that is therefore driving productivity. With more time available, AI is enabling IT teams to undertake strategic projects that can better fuel business growth and innovation.

Vitally, AI has been helping IT departments become future-ready by freeing up budgetary resources. The efficiency gains from AI have allowed organisations to allocate funds towards modernising their networks. This proactive approach is ensuring that IT infrastructure is prepared for future technological advancements, keeping the organisation ahead of the curve.

The broader enterprise perspective

While this article has used the retail industry as its core example, IoT-connected networks, driven by AI have huge potential across pretty much every industry. Hospitality, healthcare, transport, and education… all of these can realise sustainability and energy-saving benefits from the insights AI provides at every phase of operations. From procurement to resource management, smart networks can identify, leverage, and measure key sustainability factors, driving organisations towards their sought-after LEEDS certifications.

Sustainability remains a critical focus in 2025 for many of the world's enterprises. The use of AI-driven smart networks and IoT will be essential in their efforts to achieve greener operations and reduce their environmental impact.

The changing face of the workforce: is skills transformation the next digital transformation?

In 2025, the role of digital transformation continues to evolve within businesses, but there's an underlying issue – a growing digital skills gap, creating a mismatch between the digital competencies businesses require to remain competitive, and the skills their workforce possesses.

BY CASSANDRA MACDONALD, DEAN OF SCHOOL OF TECHNOLOGY, BPP

AI HAS also become a key part of the digital transformation toolbox within UK businesses. This year, AI adoption is expected to climb to 22.7%, translating to an additional 267,000 businesses leveraging the technology's solutions. However, research shows that 88% of business leaders in the UK said their staff lacked in at least one area of digital skills. This leads to challenges in innovation and growth.

As well as being a crucial business tactic designed to streamline business operations, digital transformation allows businesses to stay relevant and maintain a competitive edge whilst adapting to a fast-changing market. Without the necessary skills however, it will become increasingly difficult for businesses to adapt.

Where are the current digital skills gaps?

Digital transformation, and the increase in usage of technologies such as AI and machine learning, has marked a fundamental shift in the way that organisations ready themselves for new market demands.

To meet these new demands, it's key that workforces are equipped with the right skills. For example, although AI adoption is expected to increase by 22.7% this year, a recent survey highlighted that 33% of UK business leaders currently lack confidence in their organisation's level of AI proficiency, compared to countries such as India (49%) and France (55%). Furthermore, it's been reported that current skills gaps are forcing 43% of UK business leaders to consider hiring internationally, rather than focusing on upskilling or reskilling within their existing workforce.

How can skills gaps be addressed?

To fill these skills gaps, and reduce the need to look overseas for new hires, leaders are turning to skills transformation.

Undergoing a skills transformation involves identifying opportunities for reskilling and upskilling within the workforce and generally placing a greater focus on capabilities for greater success, rather than just looking at traditional qualifications.

As part of the ongoing skills transformation, businesses are moving away from traditional job-based planning to a more fluid, skills-focused approach, with some organisations going beyond and becoming "skills-based organisations" (SBO).

SBOs emphasise skills over traditional roles; aligning workforce planning, attraction, recruitment, professional development, performance management and talent and succession planning processes around skills needs. According to one recent report, 81% of employers used skills-based hiring in 2024 (up from 56% in 2023). But how can employers ensure that a skills transformation works to their advantage, and what does it look like in practice?

Skills mapping: creating a strong foundation for skills transformation

Working towards a skills transformation doesn't mean implementing hugely complex organisational structures. Instead, it's about having a clear understanding of the competencies needed to achieve business growth, and how to acquire, develop and deploy those skills effectively. For example, it's been predicted that more than three quarters of jobs will require some element of digital skills by 2030. With this in mind, it's vital for business leaders to take time to identify any skills gaps in the current workforce and take stock of the skills they already have.

Also known as 'skills mapping', this process will allow for purposeful team building going forward. A skills-based approach to team building means that businesses are more likely to create diverse teams with more to offer through different perspectives. As businesses evolve over time, it's also key for business leaders to recognise that skills needs are fluid. They shift and grow alongside the business, so creating clear paths for expanding capabilities is essential.

Implementing a skills strategy which makes a difference

Making more room for skills means having a robust skills strategy aligned

with overarching business strategy, which is tailored to a given organisation and its specific needs.

After mapping out the skills which currently exist within an organisation, employers must then look to prioritise hiring, partnering or training based on critical skills gaps. From there, it's essential to create a greater level of visibility for skills, by ensuring that employees understand the full range of skills required for a given role, and the opportunities there are for upskilling or reskilling where necessary.

For the digital industry, skills gaps are most prevalent in workers aged 50 and over, with 42% of employers open to hiring people in this age range, compared to 74% being happy to hire those aged 18 to 34. It's important these factors are considered within a wider skills strategy, as workers aged 50 and above could easily benefit from reskilling through the right training programme, vs externally hiring younger workers.

Another key point to take into consideration is that skills needs are fluid, and ever-changing. Scheduling an ongoing assessment of skills needs based on business progress will help to proactively identify emerging skills gaps, and how to fill them, before they become an issue for the wider business.

The crucial role of apprenticeships
Training programmes such as apprenticeships form a crucial part of any skills transformation, but some business owners question whether introducing apprenticeship programmes is the right approach for their organisation. When successfully integrated into day-to-day business operations, however, apprenticeships could lead to several opportunities for economic growth. We already know that AI usage on the rise, and businesses encouraging AI training and upskilling through apprenticeships can experience long-term cost savings, improved competitiveness, operational efficiency, more accurate decision-making, and higher employee satisfaction and retention.

To maximise impact, apprenticeships must be adequately funded and widely promoted within a business. Clear progression pathways, for example from basic digital literacy to advanced AI roles, will be essential to ensuring that the workforce is equipped with the skills it needs in the long-term.

Final thoughts

Much like the ongoing digital transformation, skills transformation has the potential to change the face of UK businesses for the better.

Skills transformation by no means must result in a drastic overhaul of the way businesses operate. Rather, understanding skills and placing more emphasis on them instead of traditional credentials, allows for a more fluid, flexible and competitive approach to business.

When implemented successfully, a greater focus on skills will allow business leaders to future-proof their workforce, as they work towards boosting economic growth in years to come.

sumup®

Digital-first strategies for growing your business, without the growing pains

The world is hyper-connected, so being 'out of date' in terms of your digital prowess is essentially a death sentence, says SumUp.

FROM STARTUPS to established businesses, having the ability to adapt and remain at the crest of the tech wave is not optional, it's a requirement.

So, if you're struggling to find your feet and get a business off the ground, then wrapping your head around the technological aspect can be a real nightmare.

Here we're going to run through some business strategies that are focused on seamlessly integrating the digital world into your business. Allowing you to grow in tandem with the technology you choose to use, from the get-go.

Let's take a look at how technology can not only improve your business but also make your work life a whole lot easier.

Make payments painless

Gone are the days of cash; actually, gone are the days of people carrying their physical bank cards around with them.

So, what has replaced this form of payment processing? Well, luckily for us it is the one thing we have with us at all times.

The era of tap to pay payments has dawned upon us.

Having the ability to accept card payments on the phone will change the face of small businesses forever. Now, our customers don't need physical money or even a physical card, and we don't need expensive machines or special systems in place.

Simply hold out your own phone, or your business phone, and let them use contactless in any way they choose. This kind of flexibility will save you hassle, time, money, and plenty of equipment, but it will also mean your customer's experience with you is efficient, secure, quick and above all, easy.

To scale a business today is to do more than just grow; scaling means expanding your operations while keeping your resources, time and money working efficiently, and taking payments with your iPhone is the ultimate example of how technology can help with this.

Spot the symptoms of 'Growth Gone Wrong' early

Scaling a business can be a tricky thing, and spotting the growing pains in business is not at all easy.

It happens to small businesses all over the world; the business starts to grow, the money begins to get better, more staff are required and before you know it, you're no longer a small business. Success seems to be just around the corner; until things suddenly get a lot harder.

Miscommunication, slow customer response, duplicated tasks and over flowing workloads can mean the destruction of a small enterprise as you transition from a small to a medium sized business.

Spotting these signs early is much easier with technology by your side, and fixing them before they affect the day to day running of your business is crucial when looking to scale your operations up.

Customer service management software, marketing technology, CRMs and workflow platforms can all help your business to efficiently manage tasks, improve communications and allow your business to grow in a controlled way.

There really is no alternative to a platform that allows your whole team to communicate, coalesce and share information.

Make the most of the incredible software that exists and make scaling a breeze.

Don't just grow: Optimise

In the light of what we just spoke about, growth is great, but if you're operating in a sub-optimal way getting bigger won't mean much.

Before you start hiring en masse, or adding more products than you can handle, take a minute and assess your current standings. Now is the time to ask yourself if your current operations are digitally optimized.

One of the key reasons businesses fail as they expand is due to them not having a good enough answer to this question.

Can your CRM scale with your pipeline? Are your payment systems up to date, mobile friendly and easy to use? Do you have adequate accounting capabilities? Do you have a way to handle onboarding?

If the answer to any of these is "No" or "I don't know", then you need to stop and address these issues while you still can, and if you need help, be sure to seek it out.

Many companies don't fully understand that they need the assistance of technology as they grow, they might need improved security, more server space, better project management tools, or even proper payment systems

without realising until it's too late. Using technology will help you shape the kind of business scale up strategy you need, in order to go from small to mighty without any costly hiccoughs.
Build a Stack That Scales With You
The right digital stack should evolve with your company, you don't need every tool on the market, just the ones that are right for you. But, before going into more detail, let's make sure we're all on the same page.

The word 'stack' is a bit jargon-ish, but bear with us.

A digital stack refers to the collection of digital tools that you use to enact your digital strategy. It simply refers to the online marketing tools you use, the accountancy applications you trust and the software that allows you to operate day to day, just as a few examples.

Your stack does not need to be extensive, you simply need the things that work for you. Here are a few great places to start.

Customer relationship management

A CRM, or Customer Relationship Management tool, essentially allows you to efficiently manage your customers' information, interaction and overall experience with your company. Contact details, marketing preferences and feedback are all contained under one roof for simple access. So, if you've got a huge client base, you'll certainly benefit from a solid CRM.

eCommerce

If you're an online business then having a scalable ecommerce store is an absolute must.

Imagine a physical shop going from 5 customers per day to, 5,000 customers per day; things would be terribly inefficient, crowded and slow.

An online store is just the same and will struggle under heavy usage without the correct servers or technical support in place. Payments will be slower, website navigation will be affected and the overall experience will be greatly reduced if your store can't cope with the traffic you receive.

Trusted online stores from the likes of SumUp, Square and Shopify offer a range of tools and functionalities designed to help brands establish a presence and grow online.

Cloud storage

In this digital age, we rely more and more on cloud storage, and it's nothing to be intimidated by; in fact, it's an incredibly useful tool. If your amount of staff increases, or you continually find you need more storage space then start searching for the right cloud storage for your business.

It will boost collaboration, streamline administrative tasks and allow every member of your team access to all the important information they need to efficiently do their jobs.

Website platform

In much the same way as your ecommerce platform, having a powerful, intuitive and aesthetically pleasing website is crucial to success in the digital age.

There are plenty of platforms out there so make sure your traffic needs are matched, and that you can use the platform to create and manage a beautiful website without any hassle.

There are many tools out there, so start off by making a list of your needs and trying to match them to the right digital tools for you; this will help you to pick the software that will serve your wider vision for how you plan to grow and scale your business.

Final thoughts: Growth without pain

Change can be a big deal. It can be scary, and things can go wrong, such is the way of the world.
But scaling up a business does not have to be scary.

With the right tech on your side it could actually be a lot easier than you might think. Growth can, and should, be exciting.

With data driven insights, maximum efficiency, streamlined operations, easy payment systems and customer focussed tools, your business could reach heights you never expected.

With these strategies in mind, you'll be able to grow and scale your business without the painful mistakes, the expensive mishaps and huge learning curve; you'll be bigger, better, smarter and more profitable before you know.

EcoStruxure™
Innovation At Every Level

Deploy your data centre FASTER with EcoStruxure™ Modular Data Centres

EcoStruxure Modular Data Centres are a smart alternative solution to overcome the traditional challenges of data centre builds.

Such as allocation of space, deployment in industrial environments, or the ability to scale capacity quickly - frees up other real estate or buildings to better support the organization's core function.

- Faster Deployment - Simplify the planning, construction, and implementation
- Flexibility to scale at a more granular level, resulting in less oversizing
- Prefabricated, pre-assembled and pre-tested in the factory prior to shipment.
- Delivered as functional building blocks of power, cooling, IT or all-in-one data centre
- Securely manage system from anywhere

Ready to get started with EcoStruxure Modular Data Centres?

se.com/datacentre

Life Is On | Schneider Electric