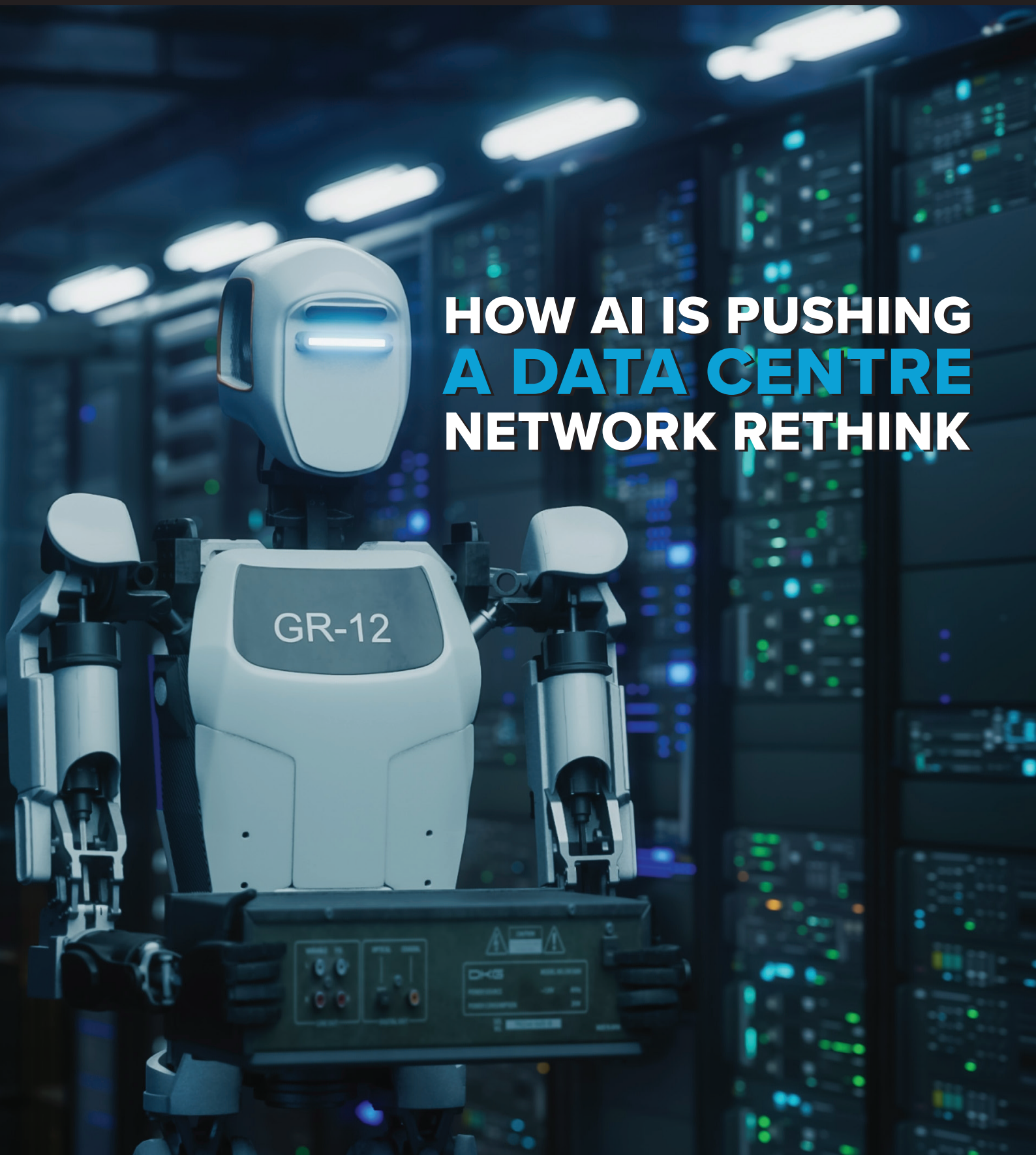
MSP CHANNEL INSIGHTS
CONNECTING THE CHANNEL PARTNER ECOSYSTEM
ISSUE V 2025
AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION
MSP-CHANNEL.COM



HOW AI IS PUSHING A DATA CENTRE NETWORK RETHINK


Liquid cooling proven at exascale.
Simplified for AI at scale.
We're ready for AI. Are you?
Learn more about our end-to-end AI-ready cooling technology
Scan the QR code to learn more.
se.com/datacentre
Life Is On
Schneider Electric

VIEWPOINT

BY PHIL ALSOP
EDITOR

Managed Services Summit London 2025 underscores industry resilience and strategic urgency

The For 15 years, the Managed Services Summit has been a fVture in the UK channel calendar. The 2025 edition, held at Convene Bishopsgate, reinforced why it remains so relevant: the ability to convene senior MSP and channel leaders around the issues that matter most - strategy, growth, security, and adaptation. The context could hardly have been more testing. With widespread Tube strikes crippling transport across London, many delegates endured commutes more than twice the norm. That over 300 decision-makers still filled the venue speaks to two things: the determination of the MSP community, and the value they place on forums that provide real-world guidance amid market uncertainty.

The programme delivered breadth and depth. Will Greenwood's keynote on resilience and leadership gave the day a unifying theme, linking the mindset required on the sports field to the realities of running MSP businesses under constant pressure. From there, technical sessions by Huntress and Defense.com cut directly into the evolving cyber threat landscape, stressing that detection-only postures are no longer defensible. Instead, remediation, response, and an understanding of attacker behaviour must sit at the core of managed security services.

Operational efficiency also featured heavily, with Umbrella, Kaseya and others providing practical levers for protecting margins while addressing customer demands for cost reduction. Sessions from ConnectWise, Sophos, Intel and ObjectFirst broadened the discussion into hyperautomation, compliance, and the practical application of AI - topics now shaping MSP operating models as much as security itself. But it was the panel sessions that generated the most debate. The M&A and Investment panel lifted the lid on

MANAGED SERVICES SUMMIT LONDON

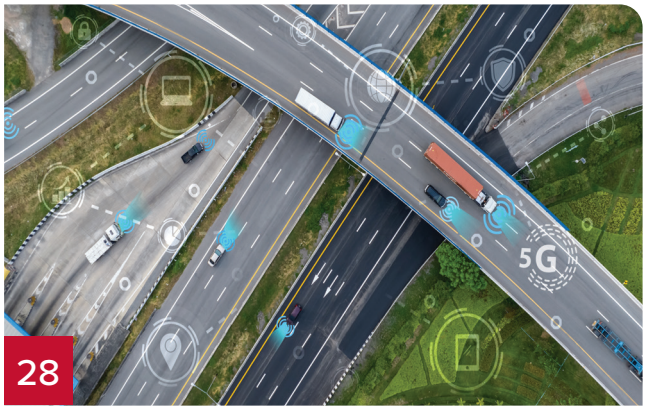
valuation trends, buyer expectations, and how MSPs can prepare strategically for acquisition or exit. For an industry where consolidation continues at pace, this transparency was both timely and necessary. Meanwhile, the vendor-free MSP Growth Panel offered something rare: operators speaking candidly about the day-to-day realities of scaling services, embedding AI, refining go-to-market execution, and driving recurring value. Delegates responded strongly, citing its immediate applicability.

That both panels resonated so strongly is telling. MSPs are less interested in theory and more in peer-driven insight that addresses operational, financial and strategic realities. The Summit succeeded by providing exactly that mV. In many respects, the logistical challenges created by the strikes amplified the event's core message: resilience is not abstract, it is demonstrated in action. The ability of the MSP community to gather, exchange, and commit to shared learning, even under difficult circumstances, reflects the sector's durability and appetite for growth.

COVER STORY

How AI is pushing a data centre network rethink

By evolving the network in tandem with the cloud, data center operators will have the foundation for a seamless and efficient continuum – one that can respond to whatever happens next in the age of AI



NEWS

MSP CHANNEL INSIGHTS

Angel BUSINESS COMMUNICATIONS

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

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

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

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

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

Directors
Sukhi Bhadal: CEO
Scott Adams: CTO

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

MSP-Channel Insights is published sV 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.

ISSN 2396-9016 (Online)

Managed Services Summit London 2025 delivers deep insight and strong community resilience

Over 300 MSP leaders gather for a day of critical strategy, technical innovation and growth oriented panels; “M&A” and “MSP Growth” panels emerge as highlight sessions.

DESPITE widespread Tube strikes across London on 10 September, the Managed Services Summit London 2025 drew over 300 senior decision makers from managed service providers (MSPs), VARs, security specialists, cloud and infrastructure vendors. Many delegates reported travel times more than doubling.

Event organisers and speakers expressed sincere gratitude for the level of commitment shown by attendees.

The event, held at Convene, 155 Bishopsgate, marked the 15th edition of the UK’s leading executive level managed services forum. It brought together a wide sponsor base – including Huntress (Headline), ConnectWise, Defense.com, Umbrella, Intel/Lenovo, ObjectFirst, Sophos, and others in Platinum and Gold tiers – each delivering sessions, masterclasses or expert panels.

Keynote, speakers & sessions

The agenda featured a blend of technical, business, security, and operational content that reflected what MSPs are facing right now. Highlights included:

- Keynote by Will Greenwood, MBE on Resilience, Triumph and Leadership, where Greenwood drew parallels between high performance sport and business under pressure – showing how leadership, teamwork and perseverance are vital for MSPs navigating rapidly changing market conditions.
- Technical deep dives such as 2025 Cyber Threat Landscape: Key Insights from Huntress (Alex Hitchen) and Be Different! Detection & Response is Not the Full Story (Oliver Pinson Roxburgh, Defense.com), both emphasising that MSPs must go beyond detection to focus on remediation, response, and threat actor tactics.
- Practical sessions on operational efficiency and cost control including Increasing Operational Margins while Decreasing Customer Cloud Costs (Gil Gross, Umbrella) and 3 Actionable Tips to Set Your MSP Up for Success in the Second Half of 2025 and into 2026 (Jack Cooke, Kaseya).
- Broader topics on cybersecurity service models, compliance, automation and AI via speakers from Sophos, Intel, ObjectFirst, and others. Sessions included Hyperautomation from ConnectWise, compliance, insurance & AI with Sophos, and Smarter AI For All by Intel.

Panel sessions that hit the pulse

Two panels, in particular, resonated deeply with the audience:

- M&A and Investment: Unlocking MSP Growth and Exit Opportunities Leaders from FluidOne, Counting Creators Ltd, Ex2 Consultancy, and Windsor Telecom unpacked where the UK MSP market stands on acquisitions, investment and exit. They discussed valuation trends, key buyer demands, and how MSPs can prepare internally and strategically for M&A. Feedback from delegates stressed how this discussion offered clarity in an area many consider opaque.
- The MSP Growth Panel – Real Strategies. Real Success Featuring MSP operators from Camwood, Nanjgel Solutions and Redcentric, this panel was vendor free and centred on real growth levers: service innovation, embedding AI, improving operations, refining sales and marketing, delivering recurring value. Delegates praised its relevance, saying it addressed issues they face day to day.

Quotes & organiser reflections

“Even when travel was difficult, seeing MSP leaders travel in made this Summit more meaningful. From the M&A session to the Growth Panel, the discussions were exactly what this industry needs right now,” said Sukhi Bhadal, CEO of Angel Business Communications.

“We set out to deliver content that matters – on leadership, AI, automation, compliance, M&A – and the audience response tells us we succeeded. Sponsors, speakers and attendees made it a day full of energy, insight, and tangible take aways.” – Sukhi Bhadal

Attendance, challenges & gratitude

The event’s success is more striking given transport disruptions: multiple Tube lines were disrupted, meaning many delegates needed to use alternative resources or allowance for delayed travel. Organisers say this reinforces how strong the MSP community is and how much demand there remains for forums like MSS where real strategy, vendor neutral content, and peer networking are central.

Looking forward

With London concluded, attention now turns to the remaining event in the Managed Services Summit portfolio:

- MSS Manchester on 18 November 2025.

The importance of independent SaaS data protection

Keepit's survey highlights the risks of relying solely on native SaaS backups, underscoring the need for independent, immutable solutions.

KEEPIT, renowned for its vendor-independent, cloud-based data protection solutions, recently unveiled the findings of its survey titled "Overlooked and under-protected: How the SaaS data gap threatens resilience".

The research underscores a significant concern: a staggering 37% of senior IT decision-makers depend purely on native SaaS backup solutions, potentially exposing their organisations to data loss and operational disruptions.

The survey, conducted in April and May 2025 by Foundry for CIO MarketPulse, received responses from over 300 IT leaders across the US, Europe, and Asia-Pacific. Their insights reveal an imperative for independent, immutable backups to ensure business resilience, highlighting potential vulnerabilities within current data protection strategies.

Key findings of the report include:

- 37% of businesses rely solely on SaaS applications' native backup capabilities, exposing them to risks.
- 11% could face recovery periods extending to a month or more, or even permanent data losses.
- 61% recognise the necessity for physically segregated storage for modern SaaS data protection.
- Nearly half (49%) experienced a major data loss event within the last year.

The alarming reliance on native SaaS backups – which typically operate under a "shared responsibility" framework—emphasises the need for third-party solutions. This approach ensures data remains protected even if access to the vendor or the user's account is lost, marking it as a recommendation by the SaaS vendors themselves.

The increasing complexity of today's threat landscape demands robust, resilient infrastructure. Data and digital sovereignty are becoming central to this conversation, prompting organisations to scrutinise vendor architecture, reliance on global hyperscalers, supply chains, and compliance with regulations.

Data and digital sovereignty are becoming central to this conversation, prompting organisations to scrutinise vendor architecture, reliance on global hyperscalers, supply chains, and compliance with regulations

Surveyed IT leaders pinpointed several critical requirements for effective modern backups:

- Physically segregated storage (62%): This ensures data independence from the SaaS provider's environment, safeguarding against platform or regional disruptions.
- Immutable, encrypted storage (59%): With end-to-end encryption, immutability offers protection from tampering or unauthorised deletion, integrated at the architecture level.
- Advanced granular access and deletion controls: Essential for compliance with GDPR and regulations like the Digital Operations Resilience Act (DORA), ensuring precise retention and deletion practices.

As emphasised by industry experts, relying solely on native backup solutions falls short in today's digital environment. Protecting data independently and immutably, while adhering to sovereignty standards, is imperative.

This control isn't merely an IT choice – it's a business necessity.

Tool sprawl: The quiet culprit behind MSP burnout

A Heimdal study reveals how the proliferation of security tools overwhelms and exhausts North American MSPs, leading to significant operational inefficiencies.

A RECENT STUDY conducted by Heimdal and FutureSafe shines a spotlight on a growing issue within the Managed Service Provider (MSP) community: tool sprawl. This phenomenon, characterised by the overwhelming number of security tools that MSPs juggle daily, is leading to operational inefficiencies, missed threats, and burnout among providers.

The survey, involving 80 North American MSPs, highlights a startling trend - the average MSP employs five security tools, with a notable 20% juggling seven to ten, and an extreme 12% managing more than ten. Of the respondents, merely 11% reported seamless tool integration, leaving a vast majority switching between multiple dashboards and engaging in laborious manual workflows.

This tool fragmentation not only contributes to fatigue but also increases the probability of overlooking genuine threats, as stated in the report. 1of 4 security alerts are meaningless with several MSPs admitting that 70% of their security alerts are false alarms, adding to the deluge of information needing attention.

Unsurprisingly, all MSPs serving over 1,000 clients confessed to experiencing daily fatigue.
The study reveals that the issue extends beyond managing alerts. The fatigue resulting from disconnected platforms bore an impact on billing processes, client onboarding, and compliance.

“Agent fatigue isn’t just a tech issue. It’s a business risk,” said Jason Whitehurst, CEO at FutureSafe. “MSPs are juggling tool after tool, but they don’t work together.”

Interestingly, while the issue is widely acknowledged, only a fifth of MSPs have opted to consolidate their security solutions. Those who have, however, report a reduction in alert volumes, improved response times, and an uplift in staff morale. Such insights underline the potential benefits of embracing a unified approach to security tools.

The research, titled ‘The State of MSP Agent Fatigue 2025’, employed a mix of quantitative analysis and thematic coding based on over 300 free-text responses to shed light on the tool integration challenges facing MSPs. You can find the report here.

Securing the future: Navigating hybrid cloud challenges

A NEW study conducted by the Enterprise Strategy Group (ESG) has highlighted the increasing challenges organisations face in securing applications within hybrid cloud environments. Commissioned by cybersecurity leader AlgoSec, the research points to the growing inadequacy of traditional network security strategies as applications become dispersed across on-premises data centres and various cloud platforms.

The report, entitled *“The Case for Convergence in Hybrid Multi-cloud, Application-centric Networks,”* reveals that an overwhelming 89% of organisations are currently using different tools and policies to secure different segments of their infrastructure. This fragmentation is complicating efforts to maintain consistent security and control across networks.
1. Hybrid Adoption: The study shows an evident shift towards hybrid models, with 85% of companies engaging two

or more cloud service providers, while 43% still keep applications on-premises. Many anticipate this distribution to persist long-term.
2. Security Siloes: Fragmentation in security tools is prominent, with nearly 80% utilising native cloud provider firewalls, alongside third-party and microsegmentation solutions. This disjointed approach compromises policy consistency and undermines visibility.
3. Increased Vulnerabilities: A significant 43% of the surveyed organisations reported experiencing a public cloud attack within the last two years, with prevalent issues such as malware propagation (44%), misconfigurations (32%), and open ports (26%).
4. Coordination Challenges: Despite some progress in integrating responsibilities for on-prem and cloud security, 55% of respondents cited insufficient collaboration among security, cloud, networking, and application teams as a key hurdle.
5. Operational Benefits: Beyond enhancing risk management, companies anticipate significant operational benefits from improved network security. The research highlights increased efficiency (63%), reduced costs (48%), and expedited cloud migrations (46%) as top advantages.

Navigate these complexities, the need for a more unified and cohesive approach to security across sprawling hybrid environments becomes evident, emphasising the urgency for strategic alignment across teams.

IT teams overconfident in resilience as outages still consume a quarter of their time

SolarWinds report suggests IT leaders underestimate the impact of broken processes and limited staff.

SOLARWINDS has released its 2025 IT Trends Report. While the findings show rising confidence in operational resilience, they also highlight that day-to-day issues continue to drain time and resources.

Based on a survey of over 200 IT professionals across Europe, including the UK, the report shows that over half (55%) of European IT leaders consider their organisation resilient, though just one in three (34%) feel it's 'very resilient'. In the UK, 44% describe their organisation as resilient, while more than half (52%) feel 'very resilient.'

Despite this optimism, the data suggests that much of this confidence could be superficial. In the UK, 44% of IT leaders spend a quarter of their working month resolving critical issues and service disruptions. Alarmingly, nearly a third (32%) report spending even more time, with an unlucky few saying up to 90% of their month is consumed by such problems. This highlights a clear disconnect between perceived confidence and the day-to-day reality of managing IT disruptions.

Crucially, nearly half of participants point to cumbersome processes, rather than technology, as the biggest hurdle to stronger resilience. Almost half of UK IT pros (49%) blame internal processes during periods of disruption, while 39% state insufficient staffing as a key barrier to resilience.

Commenting on these internal gaps between confidence and capability, Sascha Giese, tech evangelist at SolarWinds, said "This report confirms what we hear from our community and customers across the globe. Teams are dedicating real budget and effort to resilience, but many remain trapped in reactive mode. Technology alone cannot solve problems – it needs people with the knowledge and expertise, plus investment, to be able to succeed. Organisations must adopt new ways of working, in order to shift from firefighting to innovation, without compromising reliability."

Despite these hurdles, UK IT teams are taking a proactive approach and investing heavily in operational resilience. The majority (63%) report

that up to 30% of their IT budget is now devoted to disruption prevention. Across Europe, more than two thirds (69%) are upgrading tools, training and playbooks to improve internal recovery and response processes for when disruptions occur.

"In today's competitive environment, operational resilience is no longer a nice-to-have but rather a strategic imperative," added Cullen Childress, Chief Product Officer at SolarWinds. "Achieving it requires more than just adopting new technology. Organisations must equip their IT teams with the right tools, workflows, and talent to stay agile and responsive. When obstacles are removed and resilience is built into daily operations, IT becomes a true driver of competitive.

Cybersecurity skills shortage: A crisis for EMEA organisations

An escalating cybersecurity skills crisis demands a fundamental shift in organisational strategy, challenging businesses across EMEA.

A PRESSING cybersecurity skills crisis is prompting 64% of organisations in EMEA to resort to risky shortcuts and quick fixes to satisfy security demands, as highlighted in a recent report by Insight Enterprises.

In the UK, the issue is equally alarming. A substantial 67% of organisations acknowledge a cybersecurity skills gap, with over half describing the repercussions as “severe” or “significant.” The scarcity most affects senior roles, with 50% reporting deficiencies in strategic skills such as governance, planning, and risk assessment.

Across EMEA, just 24% of IT decision-makers affirm that their in-house cyber skills are sufficient to counter evolving threats. These shortages are

stalling critical initiatives (57%) and ensuring that more than half toil to meet compliance mandates.

Simplifying the dilemma to recruitment fails to capture the full scope. The cyber skills shortage is not merely a technical gap; it spans operations, leadership, and compliance, undermining resilience and long-term planning. Cybersecurity has evolved past a staffing dilemma – it is now a strategic concern. As organisations hasten digital transformation, the widening cyber skills gap is shaking confidence in their secure innovation capabilities. It’s more than a talent issue; it’s a threat to sustained growth and resilience.

Insight EMEA President Adrian Gregory emphasised a fundamental evolution in approach, stating that successful organisations are those that “ align strategic talent with intelligent technology and trusted partnerships” The key lies in leadership adept at orchestrating human–machine synergies, translating technical risks into business impacts, and embedding security in innovation. Thus, the challenge extends beyond recruitment. It calls for a reimagining of leadership approaches to cultivate resilience and maintain a competitive edge.

North East England: The new frontier for AI innovation

IN A MOVE to bolster the UK’s technological capabilities, the government has unveiled an ambitious initiative: the AI Growth Zone in North East England. This venture is projected to stimulate the economy significantly, creating over 5,000 jobs and drawing in up to £30 billion in private investment. The unprecedented partnership involves key tech players such as US-based NVIDIA and OpenAI, alongside the British company Nscale. Together, they are poised to turn the region into a central hub for artificial intelligence innovation, encompassing fields like research, data engineering, and AI safety.

Located in Blyth and Cobalt Park, the Growth Zone is geared to harness the region’s renewable energy sources and its proximity to low carbon infrastructures. This strategic position supports the establishment of major computing facilities, initiating with 8,000 GPUs, and targeting a scale-up to 31,000. This development grants researchers, start-ups, universities, and public services access to the computational power indispensable for advanced AI projects.

Beyond infrastructure, the AI Growth Zone is expected to invigorate the talent pool in sectors such as manufacturing, healthcare, energy, and finance. The initiative will leverage collaborations with local educational institutions including Newcastle, Durham, Sunderland, and Northumbria universities, cultivating a robust pipeline of skilled professionals.

The broader vision aligns with the government’s Plan for Change, striving to decentralise innovation activities away from the traditional epicentres in London and the South East.

This expansion promises to deliver a multitude of benefits, from new jobs and enhanced skill development pathways to pioneering research and infrastructure, positioning the North East as a contender for Europe’s leading AI hub.

Chris Davison, the CEO of NavLive, highlighted, “The UK’s growing investment in AI firms is fantastic news for startups. which are often the source bold innovation and agile problem-solving. These funds not only validate the strength of the UK tech ecosystem but also create space for new solutions that challenge established norms.”

“For this surge to lead to lasting impact, however, we need more than just capital. Startups need access to strong infrastructure, reliable data pipelines, and environments where they can experiment and iterate safely”

Digital adoption for UK SMEs: Navigating the platform maze

UK SMEs must embrace strategic digital adoption to unlock growth, improve efficiency, and combat platform fatigue.

UK small and medium-sized enterprises (SMEs) are accelerating their adoption of digital tools, investing heavily in software aimed at streamlining operations and boosting growth. The latest SME Digital Adoption Taskforce Final Report reveals that fragmented technology adoption can hinder productivity, with many SMEs struggling to integrate multiple platforms and manage costs effectively.

Stephen Cook, Head of Sales at Espria, highlights, “In response to specific business requirements, many SMEs have invested heavily in multiple tools. However, this is often done without consideration for integration or clear adoption strategies, which means, the very technology intended to improve efficiency becomes a source of operational drag.”

Across the UK, employees are caught juggling numerous project management systems and communication apps, each

with overlapping features. This disarray often results in lost hours switching between platforms, duplicated work, slower decision-making and increased frustration.

Market insight suggests that SMEs need a more strategic approach towards digital transformation. Understanding which platforms deliver the most value, ensuring staff are fully trained, and improving system integration are essential steps to reducing transition costs and streamlining operations.

The report stresses the need to assess the total cost of ownership, encompassing subscription fees and time costs. This evaluation is crucial for SMEs to truly understand the impact of their technology investments.

With limited resources, efficient digital adoption can create a competitive advantage for businesses.

Prioritising usability and integration over sheer tool proliferation helps SMEs avoid the pitfalls of platform fatigue, ensuring technology supports growth.

As platform fatigue gains recognition, businesses that address this issue early optimise productivity and employee engagement.

By strategically adopting digital tools and nurturing an integrated work environment, SMEs can extract tangible returns, thereby supporting sustainable growth.

Breaking down the latest IT insights

JUMPCLOUD INC. has unveiled its latest insights from commercial and mid-market organisations in the Q3 2025 IT Trends Report. This comprehensive study sheds light on the significant challenges faced by IT teams in the UK.

According to the report, only 22% of UK organisations have fully unified their IT environments. Despite ongoing digital transformation efforts, many businesses still struggle with a fragmented mix of tools. This fragmentation often results in security gaps, inefficiencies, and compliance challenges.

Respondents highlight the primary benefits of IT consolidation as improved user experience (58%), enhanced strategic focus (56%), and increased job satisfaction among IT staff (55%).

With the rapid adoption of AI, security implications are increasingly at the forefront of organisational strategies. Currently, 50% of UK organisations are evaluating Agentic AI risks while 36% are implementing new identity and access controls for AI agents.

Organisations with disjointed IT systems are more vulnerable to market fluctuations, with 46% indicating a likelihood of delaying projects compared to only 25% of those with unified systems. The report highlights the ongoing challenges of regulatory uncertainty (47%), supply chain disruptions (43%), and regional price fluctuations. Unification is deemed essential for achieving long-term resilience.

“Businesses face an expensive dilemma: their chaotic IT systems and incomplete Zero Trust efforts leave them exposed to increasing AI-driven cyberattacks,” said Rajat Bhargava, CEO, JumpCloud. “We believe that effectively navigating these complexities hinges on strategic partnerships — collaborating closely with internal teams, security leaders, and MSPs is crucial. The data clearly shows a unified, automated, and user-friendly IT foundation is the key to simplifying operations and empowering everyone’s success, even amid global uncertainty.”

Shadow AI risks proliferate as GenAI platforms and AI agents see rapid adoption

Latest research indicates increased adoption of on-premises genAI and AI agents is magnifying the challenge despite enterprises safely enabling SaaS genAI apps on a broader scale.

NETSKOPE has released new research showing a 50% spike in genAI platform usage among enterprise end-users in the three months ended May 2025. Despite an ongoing shift toward safe enablement of SaaS genAI apps and AI agents, the growth of shadow AI—unsanctioned AI applications in use by employees—continues to compound potential security risks, with over half of all current app adoption estimated to be shadow AI.

The new data was published within the company's latest Netskope Threat Labs Cloud and Threat Report. It examines the ongoing employee shift to genAI platforms, whether they are delivered from the cloud or on-premises, amid expansive interest to develop AI apps and autonomous agents, creating a new set of cybersecurity challenges that enterprises must address.

The Rise of genAI platforms

GenAI platforms, which are foundational infrastructure tools that enable organizations to build custom AI apps and AI agents, represent the fastest growing category of shadow AI given their simplicity and flexibility for users. In the three months ended May 2025, users of these platforms increased by 50%. GenAI platforms expedite direct connection of enterprise data stores to AI applications with the popularity in usage creating new enterprise data security risks that place added importance on data loss prevention (DLP) and continuous monitoring and awareness. Network traffic tied to genAI platform usage also increased 73% over the prior three month period. In May, 41% of organizations were already using at least one genAI platform. Approximately 29% of organizations are utilizing Microsoft Azure OpenAI, followed by Amazon Bedrock (22%), and Google Vertex AI (7.2%) respectively.

The many facets of on-premises AI innovation

From deploying genAI locally through on-premises GPU sources, to developing on-premises tools that interact with SaaS genAI applications or genAI platforms, organizations are evaluating many options to innovate quickly using AI, and, increasingly, they are turning to Large Language Model (LLM) interfaces.

- Today, 34% of organizations are using these interfaces, with Ollama the current clear adoption leader (33%), and others such as LM Studio (0.9%) and Ramalama (0.6%) just scratching the surface.
- Meanwhile, employee end-users are experimenting with AI tools and visit AI marketplaces at a rapid clip. For example, users are downloading resources from Hugging Face at a majority (67%) of organizations.
- The promise of AI agents is driving this behavior as the data shows there is now a critical mass of users across organizations building AI agents and leveraging agentic AI features of SaaS solutions. GitHub Copilot is now used in 39% of organizations and 5.5% have users running agents generated from popular AI agent frameworks on-premises.
- Furthermore, on-premises agents are retrieving more data from SaaS services and are doing so by accessing more API endpoints other than browsers. Two-thirds (66%) of organizations have users making API calls to api.openai.com and 13% to api.anthropic.com.

The continuation and evolution of SaaS AI use

Netskope is now tracking more than 1,550 distinct genAI SaaS applications, up from just 317 in February, indicating the rapid pace at which new apps are being released and adopted throughout the enterprise. Organizations are now using approximately 15 genAI apps, up from 13 in February. Additionally, the amount of data uploaded to genAI apps each month has increased from 7.7 GB to 8.2 GB quarter over quarter.

Ensuring AI governance and usage monitoring

CISOs and other security leaders should take necessary steps to ensure safe and responsible adoption amid the accelerated usage of varied genAI technologies. Netskope recommends the following:

- **Assess the genAI landscape:** Determine which genAI tools are in use across the organization and pinpoint who is using these tools and how they are being leveraged.
- **Bolster genAI app controls:** Establish and enforce a policy that only allows the use of company-approved genAI applications, implement robust blocking mechanisms and deploy real-time user coaching.
- **Inventory local controls:** If an organization is running any genAI infrastructure locally, review and apply relevant security frameworks such as OWASP Top 10 for Large Language Model Applications, and ensure adequate protection is in place for data, users and networks interacting with local genAI infrastructure.
- **Continuous monitoring and awareness:** Implement continuous monitoring of genAI use within the organization to detect new shadow AI instances and stay updated on new developments in AI ethics, regulatory changes and adversarial attacks.
- **Assess the emerging risks of agentic shadow AI:** Identify those who are leading the charge in the adoption of agentic AI and partner with them to develop an actionable and realistic policy to limit shadow AI.

MSP CHANNEL AWARDS 2025

CELEBRATING 16 YEARS OF SUCCESS

34 Categories across 5 Themes

3 DECEMBER 2025

LEONARDO ROYAL HOTEL LONDON CITY

KEY DATES:

3 DECEMBER: AWARDS CEREMONY

HEADLINE SPONSOR

EXAGRID®

CATEGORY SPONSORS

HORNETSECURITY

Schneider Electric

SILVER SPONSOR

Gamma

SPONSORSHIP PACKAGES

As a sponsor of the MSP Channel Awards you will gain significant marketing and branding opportunities. Sponsors are at the forefront of the awards marketing program from now until the ceremony itself in December 2025.

BOOK YOUR TABLE

Don't forget to book your table for the Awards evening. It's a great way for your company to celebrate in the run-up to Christmas.

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

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

Angel BUSINESS COMMUNICATIONS

ANGEL EVENTS

AI isn't optional anymore: how to drive adoption without diminishing trust

What happens when AI stops being a choice?

BY BURLEY KAWASAKI, GLOBAL VP OF PRODUCT MARKETING & STRATEGY, CREATIO

WELL, that moment is here. It's no longer just forward-looking tech companies that are starting to require use of AI as part of their daily jobs. Telstra - the largest telecommunications provider in Australia - has recently mandated AI usage across all of its roles, signalling that enterprise AI is no longer experimental - it's compulsory. Expect other industries to follow suit. It's not a huge surprise. McKinsey estimates AI could unlock $4.4 trillion in annual productivity gains from corporate use cases alone; in the end, it's a race and no company wants to fall behind.

But how this shift is communicated to employees will impact everything from morale to business outcomes; without the right support, it erodes confidence and autonomy. If AI is going to scale sustainably in this capacity, it needs to feel empowering rather than imposed. So how do you make this happen?

The danger of mandates without meaning

Rolling out AI across an organisation might look like progress on paper. You can install AI software on every device in your organisation, but that doesn't mean it's being used effectively or that your employees feel comfortable with it. Mandates without understanding create resistance. Especially when employees are still unsure what AI actually means for their specific roles. Will it save them time, or steal their job? These

are real concerns, and unless they're addressed openly, top-down AI rollouts risk triggering more confusion than confidence.

The answer lies in making AI adoption feel natural, not forced.

Make AI a co-worker, not a replacement

The companies seeing the most sustainable gains from AI are the ones embedding it into day-to-day workflows in ways that feel intuitive and useful. They let employees engage with AI on their own terms.

This begins with how you frame the technology. AI should be positioned as a tool that augments, not replaces, human judgment. Something that supports smarter decision-making, automates repetitive tasks and gives people more time to focus on what matters. When employees see AI as an ally rather than an adversary, they engage with it much more freely and adoption becomes much easier, and much more meaningful. And the numbers back it up. Industries more exposed to AI are already seeing three times the growth in revenue per worker compared to those less exposed.

But those gains only come when people trust the technology. Right now, there's a clear disconnect: while 54% of C-suite leaders believe generative AI is delivering value, just 35% of employees feel the same. That trust gap points to a deeper issue - the message isn't resonating where it matters most. To bridge that gap, success depends on AI tools being embedded into the systems people already use, designed with real user input, and simple enough for non-technical teams to customise and experiment with confidently.

Tools people actually want to use

This is where intuitive platforms come into play. When employees can adapt and personalise AI tools to fit their unique needs, without writing code, they're more likely to use them.

No-code agentic platforms are a key enabler here. They let users automate tasks, generate reports and build their own agentic workflows using simple visual tools: no coding required. This means no waiting for IT to get things done. This accelerates the building

of new AI capabilities, which offer intelligent suggestions, surface insights and accelerate decision-making.

It's the difference between delegation and empowerment. A sales manager can use AI to analyse pipeline health and generate personalised outreach in minutes. A compliance officer can automate audit preparation with AI-generated summaries and no-code logic.

This works because the people closest to the work maintain control.

Build adoption through culture, not just tech

This isn't just about interfaces and workflows, of course. It's about trust. Employees need to believe that the AI systems they're using are reliable, transparent and aligned with company values. This means providing visibility into how recommendations are made, ensuring regulatory compliance and maintaining human oversight. Equally important is creating an environment where teams feel empowered to experiment - without fear of failure or constant oversight. Adoption tends to take root in cultures that prioritise learning, autonomy, and gradual improvement. When people feel safe exploring new tools, embrace follows naturally. This creates the foundation for lasting change.

No-code agentic platforms are a key enabler here. They let users automate tasks, generate reports and build their own agentic workflows using simple visual tools: no coding required. This means no waiting for IT to get things done

The mandate wave is coming, but the playbook is yours

AI mandates will likely become standard practice. Once industry leaders set the pace, competitors must follow to stay relevant.

Organisations that thrive will treat AI as a mindset shift, recognising that lasting value comes from equipping people to drive change rather than forcing compliance. They'll embed AI into everyday work while respecting human expertise, encouraging collaboration and enabling smart risk-taking. As a result, it will create superior growth for the innovators who harness it. Intelligent agents will soon become core members of the enterprise workforce, and companies that fail to adapt risk obsolescence; those who lead will set the standard for an entirely new era of enterprise productivity and innovation.

The shift is accelerating. The mandates are coming. Will you be ready to implement them in ways that empower rather than alienate your workforce? Because this is what sustainable AI adoption looks like.

Shadow AI: Why businesses need better oversight of unsanctioned AI use

AI is already embedded in day-to-day workflows across most organisations, whether formally acknowledged or not. Shadow AI is a clear signal that existing governance models need to evolve.

BY JUSTIN SHARROCKS, MANAGING DIRECTOR EU/UK AT TRUSTED TECH

THE PACE of AI adoption in the workplace has far outstripped most organisations' ability to manage it. Tools like ChatGPT and Copilot are now being used across a wide range of job functions, helping teams accelerate repetitive tasks, summarise documents, or make sense of complex data. But much of this usage is happening outside formal channels, and in many cases, without IT's knowledge.

This is what we refer to as Shadow AI: the unsanctioned use of AI tools in a business environment. Unlike traditional shadow IT, which often involves people deliberately bypassing procurement or security protocols, Shadow AI tends to emerge from a lack of policy clarity or technical guardrails. Most employees are not being reckless; they simply don't realise that using consumer-grade AI tools for work could introduce significant data security, compliance and operational risks.

In some cases, however, IT teams are aware of what's being used – but simply lack the capacity or in-house security expertise to manage it appropriately. This is particularly common in lean or overstretched teams that are stuck in reactive mode, constantly putting out fires and unable to take a more proactive stance. We're increasingly seeing this skill and capacity gap widen, especially in SMBs that are facing enterprise-level demands without the same resources.

When good intentions meet poor controls

Real-world examples are increasingly common. In one instance, a junior employee at a legal firm used a free AI tool to summarise contract clauses. They weren't trying to cut corners, but in doing so, they pasted confidential client information into an external platform with no data handling agreements in place. Once discovered, this prompted a wider internal review, as the firm realised similar usage may have occurred elsewhere.

In another case, a retail store manager used Microsoft Copilot on their personal Microsoft account to automate a large portion of inventory tracking. The AI-generated files proved useful but were not accessible to others when the employee went on leave. This disrupted continuity and raised concerns about where operational data was being stored and who had access to it. Both examples illustrate how Shadow AI

can develop quietly and spread quickly, particularly when employees are encouraged to work efficiently but lack structured guidance on how and when to use AI responsibly.

Visibility is the first priority

To address Shadow AI effectively, organisations need a clear view of how AI tools are entering and being used within the business. Traditional monitoring solutions are not always equipped to detect traffic to public AI platforms, particularly when tools are accessed through personal accounts or on unmanaged devices.

Visibility can be improved through network-level monitoring that flags usage of known AI services, alongside endpoint management solutions such as Microsoft Intune, which can help enforce app access policies across both corporate-owned and bring-your-own devices. Without this level of insight, governance efforts will always be reactive and incomplete.

AI governance must be embedded in existing IT policies

Most organisations have already established frameworks for governing cloud services, setting out which tools are approved, how data should be stored, and who is accountable for oversight. These same principles should apply to AI.

An effective AI usage policy should explicitly define which tools are permitted, outline the approval process for introducing new ones, and clarify how sensitive or regulated data must be handled. It should also ensure compliance with data protection regulations such as the GDPR and assign clear responsibilities for ongoing monitoring and risk management. Importantly, these policies must be accessible and easy to interpret. If employees do not understand what is permitted or where the risks lie, well-meaning efforts to improve productivity can quickly lead to governance gaps.

Most organisations have already established frameworks for governing cloud services, setting out which tools are approved, how data should be stored, and who is accountable for oversight

Training and culture are just as critical as controls

Technical controls can only go so far without user awareness. As with phishing or cybersecurity awareness programmes, AI-related training is becoming a necessary part of enterprise risk management.
At a minimum, employees should understand which AI tools are safe to use, why certain practices – such as pasting sensitive information into public tools – pose risks, and who to approach for guidance. In the case of the legal firm mentioned earlier, the leadership team has since implemented role-specific guidance that includes practical advice on anonymising data and escalation procedures for AI-related questions.

AI governance should not sit in isolation
Shadow AI is not just an AI problem. It is part of a broader need for integrated technology governance that spans IT, security, compliance, and business operations. Once business data leaves a secure environment, there is no reliable way to know how it will be stored or whether it might be used to train external models. That loss of control poses a clear risk, particularly as regulatory requirements around AI usage become more defined.

Rather than creating a new, siloed process for managing AI, organisations should incorporate AI oversight into their existing technology governance frameworks. This allows for shared accountability, a unified risk posture, and policies that can evolve in line with both technology and regulation.

Moving forward

AI is already embedded in day-to-day workflows across most organisations, whether formally acknowledged or not.

Shadow AI is a clear signal that existing governance models need to evolve. Employees will continue to explore new tools in the absence of clear guidance, and while the intention may be to work more efficiently, the consequences can be significant: from compliance breaches to operational disruption.

Now is the time for organisations to take proactive steps. That means improving visibility into AI usage, updating governance frameworks, investing in employee education, and ensuring that AI is treated as part of the broader IT landscape – not as a standalone exception.

How AI is pushing a data centre network rethink

By evolving the network in tandem with the cloud, data center operators will have the foundation for a seamless and efficient continuum – one that can respond to whatever happens next in the age of AI.

BY ROLAND MESTRIC, HEAD OF STRATEGIC MARKETING, NETWORK INFRASTRUCTURE, NOKIA

TWENTY years ago, Jawed Karim uploaded a 19-second video to a nascent platform called YouTube. That “Me at the zoo” video triggered a massive change in the way people consume content and turned network design on its head.

Fast forward, and AI is having a similar impact today, except the effect on the cloud and network is far greater, and new app adoption is happening much faster. YouTube took three years to reach 100 million users. ChatGPT took two months.

Data volumes are pushing the outer limits of data center processing and storage capacity. The expectations around performance, reliability and security are magnitudes higher. And quality is AI’s lifeblood. While a glitch in a video can be frustrating, a glitch in an AI model can harm the validity of the result – and possibly even a client’s reputation.

The network behind the cloud isn’t top of mind these days due to other priorities such as securing the required compute capacity, ensuring a reliable and sufficient energy supply, implementing effective cooling technologies, and locking down locations. These demands are so extraordinary that industry leaders are musing about harvesting solar energy directly from space and deploying data centers on the moon.

Yet, the network will play a gating role in how far AI and the cloud can evolve. Ignoring the network risks bottlenecks by leaving expensive compute resources sitting idle while they wait for data to be transmitted between them. The cloud exists because of the network. The evolution of the cloud, whether it was to support video in the past or AI in the future, is inextricably tied to the evolution of the network.

So, what’s needed for the network to help data centers succeed in the age of AI? Let’s look first at the AI use cases that will ratchet up the pressure on a data center network.

The network-cloud continuum

Consider first centralized cloud-based gaming. When fast reaction times decide the winner, users will still choose a console over the cloud. That’s

because latency degrades performance enough that the game winner is often the one with the best connectivity. Similarly, in the future, many AI use cases are expected to require fast reaction times.

AI applications today are fairly limited and mostly text-based. Most of the AI traffic is generated to train large language models (LLMs) in big, centralized AI factories owned by hyperscalers, a few governments, research institutes, and very large enterprises.

But by 2030, 60-70% of all AI workloads will be used for real-time AI inferencing, according to McKinsey & Company.

In other words, as AI application adoption grows, the focus will shift from training to predicting and answering requests from humans, machines and agents. For mission-critical applications, this will require rapid, real-time processing and data analysis where network speed and low latency are essential.

AI workload distribution

Inferencing will also drive the distribution of AI workloads closer to the consumers of the applications. Reducing the round-trip delay will improve the overall response time of the AI models, improving the user experience and reducing bandwidth consumption.

Limiting data transmission over networks can also be critical when there are privacy and security concerns. Applications that require rapid response times or that operate in environments with limited or high-cost connectivity will benefit from distributed AI workloads.

Another perk of distributing AI workloads is the opportunity to locate data centers closer to power and cooling sources. This can make a noticeable difference in how data centers operate, helping to control costs and boost efficiencies.

Economics will also drive data center network decisions. As data centers expand and grow, cloud arbitrage will come into play. This involves dynamically running workloads on whichever cloud offers the best price-to-performance, allowing for a workload to move anywhere and at any point in the processing. Request-response fanouts determine where to find the lowest cost compute while still meeting the quality of experience required by the end user.

New needs for data center networking

While some of these use cases may seem fantastic today, the speed at which AI is forcing change makes them closer than one might think. That's because it's not just humans, or eyeballs, driving traffic – it's machines. Bot traffic accounted for 30% of all HTTP requests in early 2025, according to Cloudflare Radar data.

Sensors strapped to our bodies, probes in deep space...humans are being connected to anything and everything that can provide data. As AI agents are deployed to process this contextual information, reason, exchange data with other systems, make decisions, and act upon them in a fully autonomous way, they will generate a massive influx of data that will drive machine-to-machine communications.

With the massive challenges AI is creating within data centers around the world, the network can be a cloud's best-kept secret.

That's because connectivity is vital to how a data center functions – both inside the facility and in the wide area. Given that the network will evolve in tandem with the cloud, the transition of data centers from a centralized model out to the far edge has significant implications. Beyond the additional network capacity required to enable new use cases and AI-based applications, the network architecture needs a rethink.

Extreme speed, reliability and security will be crucial to this highly distributed, massively interconnected infrastructure to support the business and mission-critical applications that run on top of it.

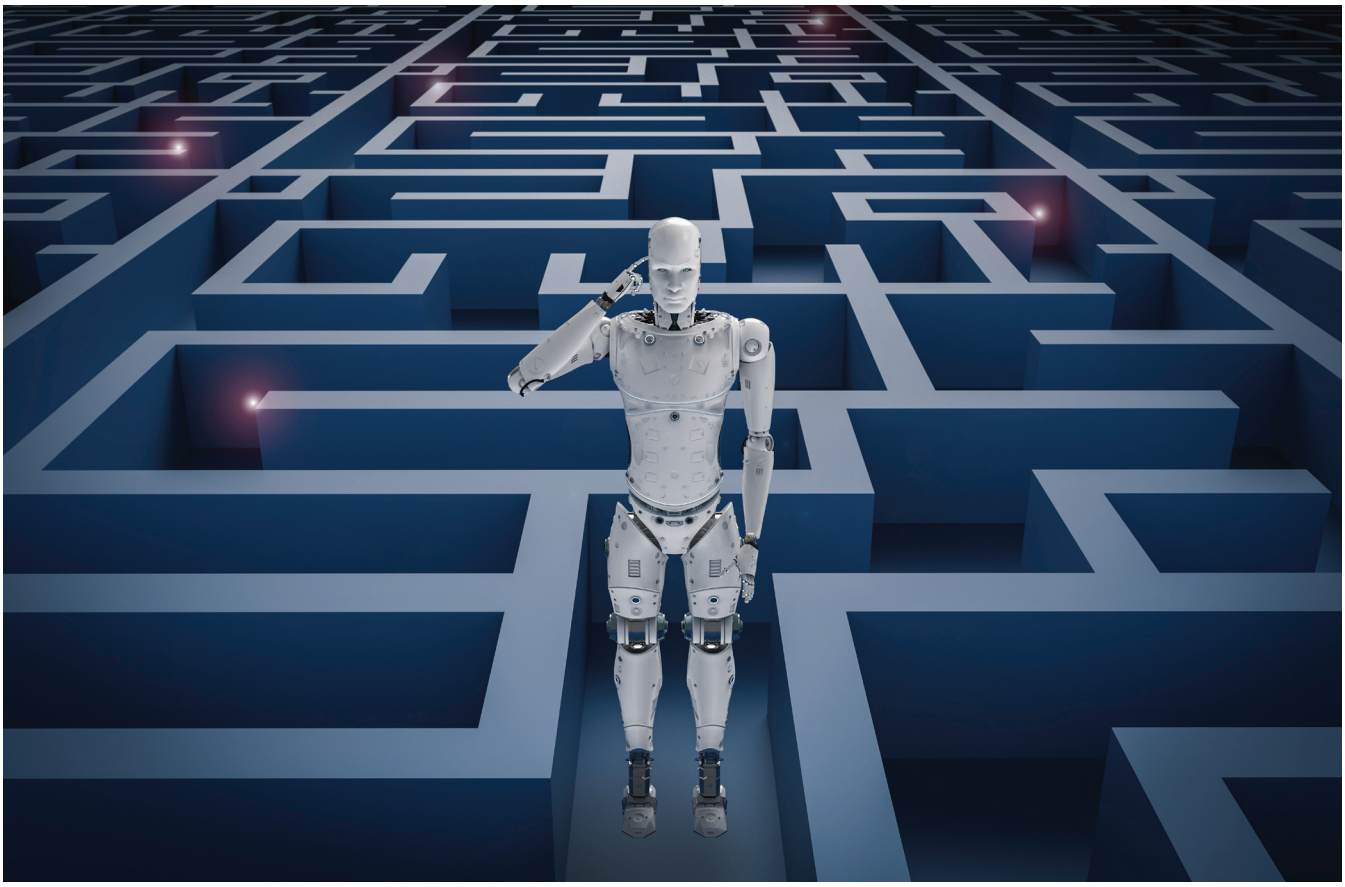
Architecting for increased scale will matter, as AI applications trigger a cascade of data requests and responses, leading to rapid traffic bursts that can overwhelm existing networks.

Network responsiveness will also be key. Robust and reliable automation will allow for dynamic adaptation as demands evolve. This is a contrast to traditional networks, which often rely on manual configurations and struggle to prioritize and allocate resources.

Network the cloud

Much like how video changed network architecture twenty years ago, AI is driving an evolution in how we think about the cloud and the network. Even with a rigorous focus on compute, power and energy, the network can emerge as a vital component of a data center's success. Evolving the network to meet the fresh demands of AI requires a visionary approach to networking within the data center itself and between distributed data centers.

By evolving the network in tandem with the cloud, data center operators will have the foundation for a seamless and efficient continuum – one that can respond to whatever happens next in the age of AI.



Guiding businesses through the AI maze

The rapid evolution of AI presents both immense opportunities and significant challenges for businesses.

BY FRANK JONES, CEO, IMS EVOLVE

ACCORDING to PwC, AI could contribute $15.7 trillion to the global economy by 2030, boosting GDP in North America by 14% and China by as much as 26%. To tap into this potential Boston Consulting Group (BCG) reports that UK business leaders plan to allocate 5% of their revenue to AI initiatives in 2025, with generative AI investments projected to rise by 60% in the next three years.

To put that into perspective, according to Statista, the average overall IT budget for an organisation is between 2-4% of revenue.

Yet, despite this enthusiasm, Everest Group research revealed that 68% of enterprises fail to achieve their desired ROI from digital transformation efforts. It is certainly true that not everything with an AI label has been a resounding success so far, even when backed by huge corporations.

The pressure to adopt cutting-edge technology though is immense, but without proper guidance, businesses risk investing in solutions that deliver superficial benefits rather than tangible value. Unlike past technological shifts, AI's iterative advancements, from large language models to computer vision, are compressing decision-making timelines. Where enterprises once had years to evaluate large enterprise-wide systems, AI tools now evolve quarterly, forcing businesses into perpetual catch-up mode.

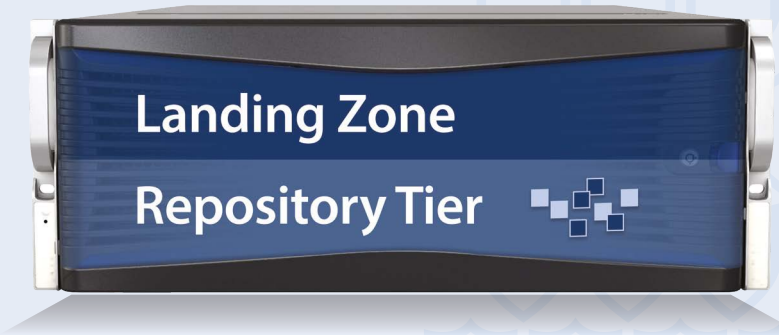
This pace of change increases the risk of 'solution fatigue,' where teams adopt disjointed point technologies without a unifying strategy. Technology providers must help clients filter noise by mapping AI capabilities to specific operational pain points, ensuring each investment delivers compounding value rather than incremental clutter.

The need for expert guidance in AI adoption

The technology sector thrives on rapid innovation, but the current pace of change is unprecedented. AI advancements are accelerating product lifecycles, making it increasingly difficult for businesses to distinguish between fleeting trends and genuinely transformative investments. In this

EXAGRID®

The future is here.
Tiered Backup Storage



- Fastest backups
- Fastest restores
- Scalability for fixed-length backup window
- Comprehensive security with ransomware recovery
- Low cost up front and over time

WINNER
SDC AWARDS 2023

- **Storage Company** of the Year
- **Backup/Archive Innovation** of the Year

Thank you so much to all who voted, and congratulations to our fellow SDC Awards 2023 winners!

Visit our website to learn more about ExaGrid's award-winning Tiered Backup Storage.

LEARN MORE >

environment, end users require more strategic direction than ever before.

Technology providers must step up to bridge this gap. Their role extends beyond supplying tools, they must act as trusted advisors, helping businesses navigate the complexities of AI integration. This means moving beyond theoretical discussions and focusing on practical, scalable solutions that align with a company's unique operational needs.

For example, AI's ability to process unstructured data and generate actionable insights could help revolutionise sales, operations, and business development. However, without expert intervention, AI models can produce inconsistent or unreliable results. Providers must ensure that AI systems are not only deployed effectively but also continuously refined to maintain accuracy and relevance.

The importance of connected ecosystems

One of the most critical yet often overlooked aspects of AI adoption is the need for connected ecosystems. As highlighted by Gartner's Hype Cycle, many AI applications are still in their early stages, leading some businesses to rush into deployment without a clear strategy.

A connected ecosystem ensures that different parts of an organisation and, crucially, different players within a supply chain, operate seamlessly. Siloed AI implementations lead to inefficiencies, inconsistent results and missed opportunities. By contrast, an integrated approach enables real-time data sharing, faster decision-making, and more cohesive workflows.

The IT sector has long understood the value of interconnected systems, where software integrations and automation streamline collaboration. However, other industries lag behind, often relying on slow, outdated upgrade cycles. In the age of AI, this is no longer viable. Businesses must prioritise connectivity to ensure their AI investments remain agile and adaptable.

Overcoming supply chain challenges

At the moment, as with all nascent technologies, most AI is being developed in silos. But when every link in the supply chain is aligned, organisations will start to realise exponential returns. If one business adopts AI while its partners do not, bottlenecks and inefficiencies will persist. As AI becomes more prevalent, the gap between adopters and non-adopters will widen, potentially leaving slower-moving businesses at a competitive disadvantage.

> A connected ecosystem ensures that different parts of an organisation and, crucially, different players within a supply chain, operate seamlessly. Siloed AI implementations lead to inefficiencies, inconsistent results and missed opportunities

Organisations need to work collaboratively to establish standardised, interoperable systems. This requires not only technological integration but also a shift in mindset, embracing AI as a collective opportunity rather than an individual advantage.

Change management and strategic partnerships

Successful AI transformation goes beyond technology, it demands effective change management. Many businesses have deeply entrenched processes that must be re-evaluated to unlock AI's full potential. This evolution must be led by experts who can analyse, adjust, and optimise workflows while ensuring minimal disruption.

Technology providers must also evolve, transitioning from vendors to strategic partners. This means developing deep expertise in specific sectors, offering tailored solutions and maintaining ongoing support to refine AI models post-deployment. Transparency is key, particularly as AI decision-making grows more complex. Businesses need clear explanations of how AI-driven conclusions are reached to build trust and ensure ethical deployment.

By taking a measured, expert-led approach, businesses can avoid the pitfalls of rushed AI adoption and instead harness its transformative potential. The role of technology providers has never been more crucial, those who rise to the challenge will not only drive their own success but also shape the future of the industry.

In an era of rapid innovation, the winners will be those who invest wisely, think long-term and build AI strategies that deliver real, sustainable value. The difference between superficial and substantive AI adoption lies in expert guidance. Businesses need partners who can deliver scalable, ethical, and strategically aligned solutions, not just the latest technology.


Liquid cooling proven at exascale.
Simplified for AI at scale.
We're ready for AI. Are you?
Learn more about our end-to-end AI-ready cooling technology
Scan the QR code to learn more.
se.com/datacentre
Life Is On
Schneider Electric

IT's moment: how AI shifts focus in the enterprise

As intelligent systems move from the periphery to the core of business strategy, IT leaders are stepping into the spotlight. What was once a back-office function is now a strategic powerhouse, guiding critical decisions at the highest level.

BY MARKUS NISPEL, CTO OF EMEA, EXTREME NETWORKS

IN FACT, 76% of UK technology leaders say the focus on AI has raised their profile at board level, up sharply from 60% just a year ago. It's a clear signal: AI is not only changing what organisations can do, but who gets to decide how they do it.

And the momentum is only accelerating. According to McKinsey, 92% of executives plan to increase their AI spending over the next three years – a move that will widen the gap between organisations embracing AI and those not.

From CIOs to VPs of IT, leaders are no longer just maintaining systems and responding to outages. They're driving innovation, shaping strategy and gaining recognition as key boardroom voices.

AI may be the catalyst, but it takes trust in its decisions, a clear understanding of how it works, and the infrastructure to support it in delivering real impact. Technology alone isn't enough.

As enterprises rewire themselves around AI, leadership must evolve too.

The platform effect

As AI adoption accelerates, enterprise networks are feeling the pressure. Nearly half of UK organisations say their network isn't ready to support large-scale AI projects.

The result? Bottlenecks that limit performance and insight, poor user experiences and strategic disconnect.

This pressure is driving a shift toward platformisation: combining networking, AI and security into a single, integrated solution. In our recent research report,

89% of executives (including 93% of CIOs and CISOs) said they want to move toward a unified approach that delivers built-in security, AI-native capabilities and seamless user experiences.

And leaders are backing it with action. 54% now rank AI deployment among their top three business priorities for 2025.

CFOs, in particular, have high expectations. More than half say poor network performance stunts business operations. They want tools that deliver ROI quickly: within quarters, not years.

Where IT was once seen as a support cost, it's now recognised as a driver of growth.

AI literacy: the new skillset of modern leadership

This shift is driving a quiet revolution in executive skillsets. To remain effective, today's C-suite must elevate their understanding of AI – not by becoming technical experts, but by grasping its strategic value, where it fits in the IT stack, and how to assess its risks and rewards.

AI isn't just another tool. It's changing how decisions are made, who makes them and what information those decisions are based on.
If you're not AI-literate, you're not future-ready.

Training builds trust

The response is heavy investment in upskilling. Our report shows 93% of execs are now training IT staff to deploy AI more effectively, with a focus on both capability and confidence in the technology.

People don't trust what they don't understand. As AI systems take on more complex decisions, building trust begins with knowledge, through transparency, reliability and meaningful human involvement.

For AI to be embraced in areas like NetOps, SecOps, and broader business operations, it must demonstrate accuracy, transparency, and security. Just as importantly, it should empower users, not replace them, by enhancing their expertise and supporting their decision-making. A conversational interface provides a good starting point, helping users retrieve information, automate simple tasks, and gradually build confidence in AI capabilities. As trust grows, users can partner with AI to extract deeper insights and eventually offload more advanced tasks. This evolution should be guided by "human in the loop" principles, ensuring users stay in control by approving, rejecting, or refining AI recommendations, maintaining oversight and accountability.

By interacting with AI, questioning responses, and seeing reasoning behind decisions, users reinforce their own understanding. AI becomes more than just a tool – it becomes a collaborator.

From assistive to autonomous

So where does this leave IT leaders? Right in the driver's seat.
As companies move beyond basic automation toward Agentic AI – systems that act independently and make complex, real-time decisions – the strategic role of IT grows even more. These aren't just efficiency tools, but agents of profound transformation. But with new power comes new complexity. Leaders must navigate everything from AI governance and data privacy to ethical deployment and regulatory compliance.

What does that look like in practice? It means building systems that are not only powerful but also explainable, auditable and secure.

Finally, a seat at the table

AI has given IT a rare opportunity to redefine its value as a strategic partner. The boardroom is holding the door open.

The organisations that thrive in this next chapter will deploy AI quickly. But more importantly, they'll be the ones that integrate it wisely and put it in the hands of those best equipped to lead.

In the age of AI, IT is finally taking its seat in the boardroom.

And ultimately, the enterprises that thrive will be those where technology leaders are empowered, strategic, and AI-literate.

AI isn't just another tool. It's changing how decisions are made, who makes them and what information those decisions are based on. If you're not AI-literate, you're not future-ready

Transforming cyber defence with Agentic AI

gentic AI marks a critical shift in how cyber professionals tackle increasingly sophisticated and complex threats.

BY MICAH HEATON, EXECUTIVE DIRECTOR, MICROSOFT SECURITY CENTRE OF EXCELLENCE AT BLUEVOYANT

WE HAVE entered a dangerous phase in cyber security marked by the rise of deepfakes, polymorphic phishing schemes, and AI-driven reconnaissance tools that are now both accessible and highly effective.

The expense of launching an attack has significantly decreased, enabling untrained threat actors to create increasingly sophisticated attacks that breach user security, infiltrate infrastructure, and extract valuable data in just hours instead of days.

At the same time, the cost of defending a company's perimeters remains constrained by budget cycles, compliance requirements, and multiple levels of change control. Security teams are often burdened with the impossible task of sifting through large amounts of data to detect signs of a security breach. This is true of 85% of analysts who spend substantial time gathering evidence to turn an alert into a usable security case.

This ultimately constrains security teams' ability to focus on more urgent security issues and threats. Therefore, these teams must begin offloading and automating some of these processes to ensure better accuracy and efficiency when navigating the complex threat landscape.

Introducing Agentic AI

This is where Agentic AI steps in as part of an established Managed Detection and Response (MDR) solution, enhancing the role of the analyst rather than replacing them. Agentic AI acts autonomously, making decisions rather than simply assisting while continuously learning and improving over time. This can assist in offloading the burden of tasks that security teams are inundated with.

Human involvement in threat investigations can lead to costly errors and inconsistencies for organisations. Agentic AI is changing this dynamic by taking independent action, using machine learning to triage, investigate, respond, and escalate issues at machine speed. This technology enhances the detection and response to high-value threats with greater accuracy, while minimising human error.

Agentic AI in action

Agentic AI isn't just a theory; it is already reshaping how security operations centres (SOCs) detect and respond to threats. Agentic AI provides critical insights that might be overlooked due to user errors and

misconfigurations. Monitoring the threat landscape 24x7, Agentic AI tools ensure timely escalation and support for security incidents, particularly when human teams may be less vigilant or response times are prolonged.

Other Agentic AI capabilities include:

- Auto-prioritisation of alerts ranks alerts by considering the risk context rather than relying on predefined severity scores.
- Case summarisation analyses and learns from the behaviours of top analysts to enhance decision-making and efficiency.
- Response recommendations offer actionable suggestions for responding to incidents, complete with supporting evidence to facilitate faster resolutions.
- Threat hunting queries are generated, fine-tuned, and executed proactively, eliminating the need for analysts to wait for a formal ticketing process to begin investigating potential threats.

Speed without losing control

While the demand for speed is essential as security teams manage the evolving attack landscape, it must not come at the expense of accountability and responsibility. Agentic AI models must operate with user control, transparency, accountability, and explainability in mind, as per the guidelines below:

- **User Control:** Provides human experts with the ability to define the appropriate level of automation for their operating and business environments. Users can decide when to relinquish control to automation and when to override it in case of any errors to avoid impacting business and service continuity.
- **Transparency:** Any actions taken by the system using artificial intelligence should provide reasoning and references to the data points that were used and clear identification of when AI is in use.
- **Explainability:** Provides extensive information on the process of generating AI produced content, instilling confidence in the content.
- **Accountability:** Ensures AI and AI powered features are accountable, making the natural interlacing of human and machine actions easily distinguishable for reporting or auditing.

Redefining AI in cyber security

Agentic AI marks a critical shift in how cyber professionals tackle increasingly sophisticated and complex threats. It empowers analysts to move beyond responding to alerts, allowing them to instead focus on high-level decision-making and innovative, strategic thinking.

By redefining the existing rules of engagement between AI and cyber security, organisations can effectively navigate complex cyber security challenges and safeguard their networks against potential breaches and attacks, at a time when the financial, legal, and reputational stakes have never been higher.

In doing so, businesses can maintain a competitive edge, enabling them to remain one step ahead of malicious actors.

Unlocking scalable infrastructure with Agentic AI

From automation to autonomous – how agentic is shaping the future of network infrastructure.

BY GARY SIDHU, SVP PRODUCT ENGINEERING AT GTT

WE HAVE entered a new era. One where software can operate autonomously and proactively within its environment. It can make independent decisions, implement them, and continuously learn from its experiences.

Simply put, agentic AI listens, learns, and develops strategies capable of revolutionising how we work, especially in network operations where it shifts from reactive to proactive, improving resilience and security. It can automate network management, real-time threat detection, and traffic optimisation, enhancing efficiency, strengthening security, and boosting network performance for seamless and secure operations.

But how can it be implemented, where can it have the biggest benefit, what is the role of human oversight and what lessons can we learn from the introduction of agentic AI? In this article, I'll cover these key points and give advice to businesses looking to harness its potential.

Setting the foundations for agentic AI

The successful implementation of agent-based AI systems requires careful planning.

Firstly, it is important to clearly define goals and key performance indicators for their use. Then, a major challenge is the seamless integration of the

solutions into the existing IT network infrastructure. Training and operation of the systems also require the availability of sufficient and high-quality data. Finally, there are ethical considerations of implementing agentic AI that companies need to address from the outset, such as data privacy, protection, governance, human oversight and transparency, to ensure trust is built.

Agentic AI requires guidelines over which data it can access, from where, and whether it is able to share certain data externally. This is imperative to consider within an AI strategy to ensure both customer and organisational protection from data and regulatory breaches, particularly in the light of regulations such as the EU AI Act.

If your implementation plan takes these considerations into account, nothing stands in the way of the effective use of agentic AI. With digital agents, businesses can streamline their operations, meeting rising customer service expectations. A report by Gartner predicts that by 2029, AI will resolve 80% of common customer service issues without human intervention. These agents analyse customer sentiment in real time and provide tailored responses enhancing customer engagement.

From monitoring to action: AI in network infrastructure

Agentic AI is now playing a pivotal role in network infrastructure and cybersecurity, helping organisations

move beyond traditional, rule-based systems. Unlike conventional tools that passively monitor and alert, digital agents can actively observe network behaviour, identify anomalies in real time, and take autonomous action to resolve emerging threats. This enables a faster response to incidents, reducing downtime, and therefore helps avoid costly disruptions.

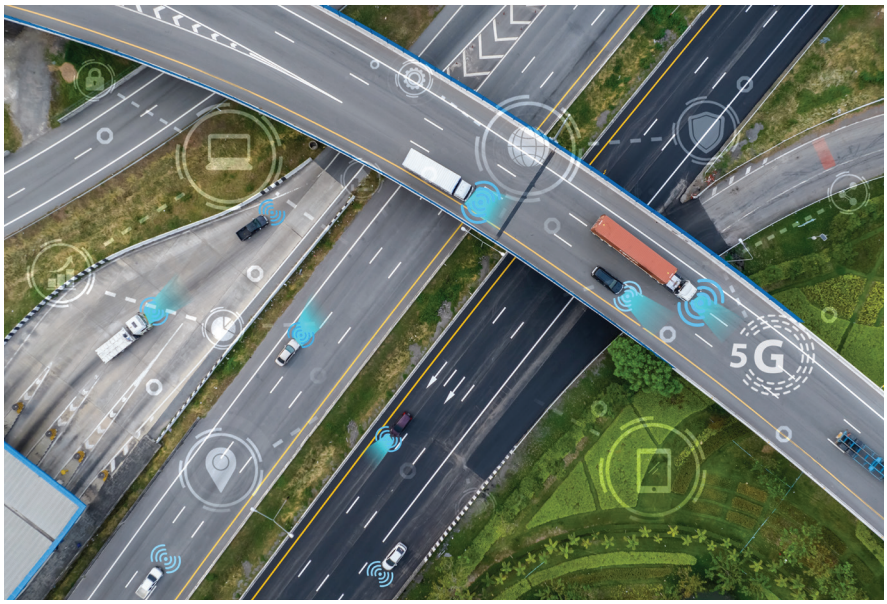
Agentic AI is already being embedded across networking and security infrastructure to deliver real-time, measurable value. The NSaaS model (Networking and Security as a Service) is evolving into something more dynamic, where agentic capabilities enable smart routing, adaptive policy enforcement, and predictive resource allocation. These enhancements ensure better performance, greater visibility, and stronger protection for global customers operating in complex conditions.

Breaking down siloes in operations
There is growing demand for integrated cybersecurity and networking solutions from cloud providers, with many organisations viewing this convergence as essential to enterprise resilience. In this setting, agentic AI offers a unique advantage; it blends machine learning with autonomous decision-making, allowing digital agents to adapt in real time while maintaining stable and efficient network operations.

This shift from static systems to intelligent, self-improving agents is reshaping how businesses think about their digital foundations. With this strategic mindset, early adoption of agentic AI gives network providers a chance to get ahead of the curve with smarter services, improved reliability, and a more personalised customer experience.

Maximising value

While we are still at the beginning of the AI journey and its potential is yet to be fully realised, McKinsey found that 77% of companies are either using AI or exploring its potential. It has already changed workflows, it still requires a level of human management, but agentic AI enables new possibilities.



It can become more than a support tool. It can become an active participant in business operations, freeing up resources and creating greater efficiency. In networking specifically, the benefits are becoming clear.

While machine learning has been used for tasks like digital twins and anomaly detection, agentic AI can manage these processes autonomously. This reduces the need for human intervention at every step and enables networks to become more resilient, secure, and adaptive to real-time demands.

Nevertheless, learning and development around AI in the workforce remains a business imperative. Counterintuitively, while flawed data is often tolerated in human decision-making, we don't have the same leniency with AI. According to Gartner, 30% of generative AI projects are abandoned after the proof-of-concept stage, primarily due to issues related to data quality, risk management or high costs, highlighting the difficulty organisations face in AI initiatives and importance of getting implementation right from the off.

For some companies, agentic AI could mark a shift from promise to performance - where AI becomes not just an experiment, but a business-critical capability aligned to strategic goals.

Infrastructure that adapts and protects

For business leaders, agentic systems offer a new path. They align technology with strategic goals and turn intelligent automation into a core business enabler.

For organisations ready to move from passive AI to proactive systems, agentic could serve as the intelligent enabler. This is not just a technological shift, but a reimagining of what network infrastructure can achieve when paired with AI designed to think, act, and adapt.

Agentic AI is now playing a pivotal role in network infrastructure and cybersecurity, helping organisations move beyond traditional, rule-based systems. Unlike conventional tools that passively monitor and alert, digital agents can actively observe network behaviour, identify anomalies in real time, and take autonomous action to resolve emerging threats

Simplifying cybersecurity: a strategic imperative for the digital age

As the world becomes more digital, the stakes will only rise. But with a streamlined and strategic approach, tech leaders can turn cybersecurity from a reactive cost centre into a proactive enabler of business.

BY ARTUR MARTINS, CISO | CYBERSECURITY STRATEGY EXECUTIVE ADVISOR, LOGICALIS

ACROSS INDUSTRIES and borders, the scale and frequency of cyberattacks are accelerating. From ransomware to supply chain vulnerabilities, the digital threat landscape is evolving faster than many organisations can keep up with. To meet this rising tide of risk, businesses have responded in the most natural way possible, by investing. New tools, new platforms, and new services have been added to the stack at pace, each promising improved protection.

But somewhere along the way, this well-intentioned investment has become overly complex. And this complexity is now becoming one of the biggest cybersecurity threats facing organisations.

According to the Logicalis 2025 CIO Report, over half of CIOs now say their cybersecurity environments are too complex to manage effectively. These systems, once built to protect, are now creating risk by their very design. In fact, 50% of tech leaders admit they are not getting value from their security tools because they are not using most of the features. These numbers reveal a sobering truth - complexity is eroding control, visibility, and confidence.

Security sprawl is creating more problems than it solves

The rise of security sprawl has been gradual but relentless. As new threats have emerged, organisations have bolted on point solutions to address

specific gaps. Cloud migration, remote work, third-party ecosystems and regulatory changes have all added layers to an already fragile foundation.

What results is often a patchwork of disconnected tools from multiple vendors, with overlapping functions and different management consoles. This not only increases the operational load on security teams, but also introduces blind spots where threats can hide undetected. The Logicalis report highlights that only 58% of CIOs are confident in their ability to identify potential security gaps. In an environment where cyberattacks unfold in minutes, that lack of visibility can be costly. Rather than helping IT leaders sleep better at night, bloated security stacks are keeping them up.

Simpler systems are stronger systems

Simplifying cybersecurity is not about reducing protection; it is about removing unnecessary friction and focusing on what truly matters. When security architecture is streamlined, organisations gain better situational awareness, faster response times, and clearer decision-making pathways.

The first step is often a full assessment. CIOs and CISOs need to ask hard questions about their existing environment. What are we protecting? Where are our biggest risks? Which tools are underused or redundant? Are any processes creating delays or confusion during incident response?

From this point, a path forward becomes clearer. Three strategies in particular are helping organisations modernise their security posture in a more sustainable and effective way.

1. Consolidating where possible

Tool consolidation is a practical and high-impact first move. Integrated security platforms can help reduce complexity by managing multiple risk domains from a single interface. These platforms often include capabilities like threat detection, endpoint protection, network monitoring, and identity access management within one unified system.

This approach improves visibility across the environment, simplifies configuration, and reduces the number of tools and vendors IT teams need to manage.

Consolidation also supports the shift from reactive to proactive security. By breaking down silos, teams can spot and act on early warning signals faster.

2. Embrace automation and orchestration

Manual processes remain one of the weakest links in enterprise cybersecurity. From patching to threat detection and response, tasks that require human intervention are not only time-consuming but prone to error. Automation offers a powerful solution.

By introducing automation for routine tasks, IT teams can shift their focus toward higher-value activities like threat analysis, policy refinement, and strategic planning. Automated workflows also improve consistency in incident response and make it easier to meet growing compliance requirements.

Security orchestration, which connects and coordinates tools across the ecosystem, further enhances this approach by enabling fast, cohesive action across systems when incidents occur.

3. Engage specialist partners

Cybersecurity is no longer something most businesses can manage alone. The threat landscape has become too sophisticated, and the talent shortage too severe. Partnering with managed security providers gives organisations access to advanced capabilities, 24/7 monitoring, and expertise that may not be available in-house.

Outsourcing functions like threat intelligence, security operations centre services, and incident response can improve resilience while allowing internal teams to focus on innovation and transformation.

Why this matters now

There is more than operational efficiency at stake here. As governments and regulatory bodies around the world tighten their expectations on data protection and cybersecurity governance, organisations must be prepared to demonstrate accountability. The rise of legislation like the EU's AI Act and ongoing updates to data privacy laws demand clear, auditable records of how systems are secured and maintained. This is nearly impossible to achieve in environments that are sprawling and disjointed. Simplification supports compliance by enabling cleaner reporting, faster audits, and more transparent controls.

A future-ready security strategy starts today

The CIO's role in security has never been more strategic. As the lines between risk, resilience, and reputation continue to blur, the pressure is on to lead with clarity and purpose. Simplification offers a way forward.

By rationalising tools, embracing automation, and leaning on expert partnerships, organisations can shift from complexity to confidence. This is not just a technical evolution but a mindset change — one that recognises that the goal of cybersecurity is not to do more, but to do what matters, better.

As the world becomes more digital, the stakes will only rise. But with a streamlined and strategic approach, tech leaders can turn cybersecurity from a reactive cost centre into a proactive enabler of business.

The MSP evolution: building flexibility and choice into licensing models

Managed Service Providers (MSPs) have long operated in a landscape shaped by vendor licensing models, which have often been quite rigid and have become increasingly monopolistic. Recent developments, particularly the strategic shifts by Broadcom and Citrix, have intensified pressure on MSPs, forcing many to reevaluate their infrastructure strategies and partner relationships.

BY BEN COLMAN, WHOLESALE REGIONAL PARTNER MANAGER FOR EMEA AT 11:11 SYSTEMS

BROADCOM'S acquisition of VMware brought sweeping changes to the VMware Cloud Service Provider (VCSP) programme, changing long-standing licensing structures and pricing models. Similarly, Citrix, now under the Cloud Software Group (CSG) following its merger with TIBCO Software and acquisition by Vista Equity Partners and Evergreen Coast Capital, has moved away from its 'channel-first' model. The company now focuses on direct sales to the top 1000 enterprise accounts, leaving smaller MSPs sidelined and redirected to top-tier distributors, many of whom lack the agility or technical depth to support them effectively.

Disruption as a catalyst for innovation

While these shifts have created short-term challenges, they also present a unique opportunity for MSPs to evolve. The traditional model, where MSPs owned every layer of service delivery, from infrastructure to software licensing, is giving way to more flexible, scalable approaches. MSPs are increasingly embracing hosted platforms and wholesale infrastructure models that support multi-cloud environments like AWS, Azure, and Google Cloud.

This evolution allows MSPs to reduce capital expenditure, streamline operations, and regain control over

their service stack. By shedding the burden of proprietary data centres and rigid vendor contracts, providers can deliver better outcomes for clients and avoid being locked into vendor-driven pricing models. It is a win-win scenario: MSPs gain agility and cost-efficiency, while customers benefit from improved reliability, broader geographic coverage, and modern management tools.

The rise of the wholesale MSP model

One of the most transformative trends in the MSP space is the rise of the wholesale model. This is where MSPs procure infrastructure services from vendors such as 11:11 Systems and offer it under their own branding. This model offers unmatched flexibility, scalability, and control over the customer relationship.

Rather than beholden to vendor licensing terms, MSPs can tailor services to meet the specific needs of their clients. They can scale rapidly, integrate specialised solutions, and offer enterprise-grade services without the overhead of managing physical infrastructure.

This shift empowers MSPs to focus on innovation and customer experience rather than navigating complex vendor ecosystems.

How the MSP landscape has evolved

This wholesale model aligns well with how the MSP industry is evolving. In recent years it has undergone significant transformation, driven by several key factors:

- **Cloud Adoption:** The widespread adoption of cloud computing has fundamentally changed how MSPs deliver services. Traditional on-premises models are being replaced by SaaS, hybrid and multi-cloud architectures, enabling greater flexibility and scalability.

- **Security Demands:** With cyber threats on the rise, MSPs are increasingly expected to provide robust security solutions. This has led to the emergence of Managed Security Service Providers (MSSPs) and the integration of advanced threat detection, compliance, and incident response capabilities.

In this evolving and shifting environment, 11:11 Systems has emerged as a trusted partner for MSPs seeking stability and growth. By offering wholesale infrastructure access, seamless workload migrations, and a robust global platform, 11:11 Systems helps MSPs navigate vendor changes with confidence

- **Automation and AI:** Automation tools and AI-driven platforms have enabled MSPs to improve efficiency, reduce manual workloads, and deliver proactive support. Predictive analytics, self-healing systems, and intelligent monitoring are becoming standard offerings.

- **Customer Expectations:** Clients now demand more than just uptime, they expect strategic guidance, seamless integration, and continuous innovation. MSPs must evolve from service providers to trusted advisors.

- **Vendor Consolidation:** Mergers and acquisitions among major vendors have reshaped the partner landscape. As seen with Broadcom and Citrix, these consolidations often lead to tighter control over licensing and reduced support for smaller partners.

In this evolving and shifting environment, 11:11 Systems has emerged as a trusted partner for MSPs seeking stability and growth. By offering wholesale infrastructure access, seamless workload migrations, and a robust global platform, 11:11 Systems helps MSPs navigate vendor changes with confidence.

A new ecosystem of resilience and choice

The MSP evolution is not just about technology; it is about building a new kind of ecosystem. One that values resilience, customer experience, and scalable growth. As MSPs move away from vendor monopolies and embrace flexible models, they are better positioned to meet the diverse needs of modern businesses.

This shift also encourages innovation. Freed from rigid licensing structures, MSPs can explore new service offerings, expand into untapped markets, and deliver tailored solutions that drive real business outcomes. For customers, this means more choice, better service, and a stronger foundation for digital transformation.

The ability to pivot, adapt, and innovate in response to market changes is now a key differentiator. MSPs that embrace this mindset will not only survive but thrive in this new landscape. Whether you are a partner navigating vendor transitions or a customer seeking reliable cloud solutions, the message is clear: flexibility, choice, and strategic alignment are the pillars of future success.

The MSP industry is at a crossroad. Legacy models are being challenged, and new paradigms are emerging. The wholesale MSP model, supported by partners like 11:11 Systems, offers a compelling path forward, one that prioritises agility, customer ownership, and scalable growth.

As the landscape continues to evolve, MSPs must remain vigilant, proactive, and open to change. By doing so, they can turn disruption into opportunity and build a future-ready business that delivers lasting value for their customers.

A cautionary tale from the frontlines of cybersecurity

Cybersecurity breaches don't always come from external threats. Sometimes, the risk is sitting at one of your own desks - or working remotely from halfway across the world.

BY NADEEM AZHAR, CEO OF PC.SOLUTIONS.NET

AT a mid-sized manufacturing company in Texas, one of their employees quietly outsourced his entire job to an offshore contractor. Without the company's knowledge, he paid someone overseas to perform his day-to-day responsibilities while he collected a full paycheck and focused on other personal projects.

The scheme went unnoticed for months. IT didn't flag it. HR didn't see it. Not even the employee's direct supervisor suspected anything was off. The truth only surfaced when the offshore contractor stopped getting paid and threatened to leak sensitive company data.

This wasn't a criminal hacker or a ransomware gang. It was a freelancer with access to production specs, machine data, and internal systems – someone with no background check, no NDA, and no formal relationship with the company.

If that doesn't make business leaders stop and rethink their internal controls, it should.

The real risk isn't just tech – it's trust without process

This incident highlights a blind spot we see too often: many companies invest in strong firewalls, antivirus solutions, and VPNs—but neglect to audit who has access, how roles are monitored, and whether job responsibilities match system behavior.

Cybersecurity isn't just about preventing outside intrusions. It's about ensuring internal alignment, accountability, and oversight. Especially in industries like manufacturing and logistics, where production data and vendor specs are business-critical, unauthorized access or data exfiltration can result in more than just reputational damage. It can bring operations to a halt, violate contractual obligations, and destroy competitive advantage.

Five steps every company should take immediately:

- **Audit access rights.** Review who can log into what – and remove dormant or mismatched access.
- **Align systems with roles.** Make sure the tools people access match their actual responsibilities.
- **Monitor behavior, not just logins.** Track for anomalies in usage patterns that might suggest fraud.
- **Create a culture of internal reporting.** Team members should feel safe flagging unusual behavior without fear of retaliation.
- **Partner with IT teams who understand your industry.** Cybersecurity isn't one-size-fits-all – manufacturers face different threats than law firms or clinics.

Houston Businesses Are Not Immune
As a cybersecurity provider based here in Houston, I've seen firsthand how quickly trust can become a vulnerability.

As companies continue to embrace hybrid work, global talent, and digital tools, internal oversight must evolve to keep pace.

The question isn't whether your systems are secure from outside attack. The question is whether they're built to catch the threats already inside your organization.

And in this case, the cost of not knowing was almost everything.

MSP CHANNEL AWARDS 2025

CELEBRATING 16 YEARS OF SUCCESS

34 Categories across 5 Themes

3 DECEMBER 2025

LEONARDO ROYAL HOTEL LONDON CITY

KEY DATES:

3 DECEMBER: AWARDS CEREMONY

HEADLINE SPONSOR

EXAGRID®

CATEGORY SPONSORS

HORNETSECURITY

Schneider Electric

SILVER SPONSOR

Gamma

SPONSORSHIP PACKAGES

As a sponsor of the MSP Channel Awards you will gain significant marketing and branding opportunities. Sponsors are at the forefront of the awards marketing program from now until the ceremony itself in December 2025.

BOOK YOUR TABLE

Don't forget to book your table for the Awards evening. It's a great way for your company to celebrate in the run-up to Christmas.

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

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

Angel BUSINESS COMMUNICATIONS

ANGEL EVENTS

Gammaverse 2025: Partnership, Progress, and a Touch of Pirate Spirit

THE ENERGY inside London's Queen Elizabeth II Conference Centre was undeniable. From the moment Gamma Business Managing Director Will Morey opened Gammaverse 2025, it was clear this was not a typical vendor event.

"This isn't about platforms or products or portals," Morey told the packed audience. "It's about how we can build stronger businesses, stronger partnerships, and drive stronger growth for the whole channel."

That tone, collaborative, human, and forward-looking, shaped a day that celebrated both innovation and community in equal measure.

Webex for Gamma Takes Centre Stage
While Gammaverse is known for focusing on relationships, not roadmaps, there was still excitement around one of the most anticipated product moments of the year: the official launch of Webex for Gamma.

As part of Gamma's expanding UCaaS portfolio, Webex for Gamma represents a new era of collaboration and customer experience technology.

Together with Horizon with Webex, it provides partners with two distinct routes to market, complementary rather than competitive, and both built to meet customers wherever they are in their communications journey.

"Webex for Gamma isn't just a product, it's an opportunity," said Andrew Robinson, Gamma's Head of UCaaS Practice. "It enables our partners to deliver advanced collaboration and AI-driven customer experiences without compromising on reliability or simplicity."
That sentiment was echoed by John Murphy, CEO of Gamma Business, who described the dual Webex offerings as "two paths that move forward together."

Delegates were shown how embedded AI capabilities like smart audio, live transcription, and real-time call summaries are making collaboration smarter and faster, not by replacing people, but by freeing them to focus on meaningful interactions. Lauren Williams, UCaaS Sales Specialist, summed it up neatly: "These aren't just features. They're the details that make every conversation count."

The integration of Webex into Gamma's ecosystem also brings new customer experience capabilities via Cisco's Webex Contact Centre. Features like sentiment analysis and automated follow-up are designed to ensure "every interaction is handled with confidence."

It is a move that not only modernises Gamma's UCaaS suite but reinforces its broader strategy of giving channel partners enterprise-grade tools with flexible commercial options.

Innovation beyond technology

If the Webex launch provided the "what" of Gammaverse, then the day's keynote speakers explored the "why."

First up was Sam Conniff, the entrepreneur and author behind Be More Pirate. Conniff's session set a tone that was part provocation, part invitation. He urged the audience to question long-held assumptions about success and leadership, and to start "professionally breaking the rules."
"The rules we inherited aren't always the rules we need to follow," Conniff told delegates. "True progress comes from those willing to challenge convention and rewrite the code."

His talk connected deeply with the audience, especially in a channel environment where creativity often thrives within the constraints of process. Conniff pointed out that history's original pirates weren't anarchists but innovators. "They built their own codes of conduct and designed fairer systems than the empires they fought against," he said.

For him, piracy wasn't about chaos but about community, a key message that landed strongly with Gamma's audience. "No matter the problem," Conniff said, "the answer is always community."

That idea of connection and shared progress tied neatly back to Gamma's Edge framework, its partner-led growth programme designed to bring tools, insights, and support together under five key pillars. As Morey later observed, Gamma's role in the channel is increasingly about co-creating new models rather than dictating them.

"Rule breaking, in our world, is about innovation," Morey commented after the session. "It's about listening to partners, finding new ways of working, and refusing to get stuck on the tracks of success."

The evolving edge

The theme of listening and acting ran through the day's other sessions. Holly Mack, Gamma's Business Planning Director, gave delegates a closer look at the company's Voice of the Channel initiative, a structured listening programme gathering partner feedback to help shape everything from pricing to enablement.

"It's not a one-off survey," Mack explained. "It's an ongoing conversation that will evolve our strategy and strengthen how we work with partners." That commitment to data-driven decision-making was reflected again in CTO Colin Lees' demonstration of Gamma's modernised partner portal. Redesigned for speed and clarity, the new portal integrates richer data insights, giving resellers a complete view of their customer estate and shortening the time it takes to bring new products to market.

"Technology has to solve customer problems," Lees said. "If it doesn't make partners' lives easier, it's not doing its job."

The showcase also highlighted the evolution of SafeWeb Pro, Gamma's cyber security solution for SMBs, now with optional insurance coverage working with Chubb, and reaffirmed the company's investment in iPECS Cloud for customers continuing their voice migration journeys. Taken together, the message was clear: Gamma's innovation strategy is guided not by what is fashionable, but by what helps partners grow.

Lessons in Leadership: Joe Marler steals the show

If the morning inspired reflection and collaboration, the afternoon brought laughter and plenty of it.

Enter Joe Marler, former England and Harlequins prop, podcaster, and self-proclaimed "attention-seeking narcissist." In conversation with Gamma Channel Director Matt Barnett, Marler delivered what may be one of the most colourful keynotes ever heard at a technology event. But beneath the humour was genuine insight. Marler spoke candidly about reinvention, team culture, and mental resilience, the same qualities that drive high-performing teams in sport and business alike.

He described the camaraderie of the rugby world, the challenges of leadership, and the need to "find an environment where everyone pulls together for a common goal." His reflections on belonging, honesty, and failure resonated deeply with an audience that knows the importance of collaboration in tough markets. "Everyone plays their part," Marler said. "Everyone is part of something bigger than themselves."

For many, it was the standout moment of the day, a reminder that authenticity and teamwork remain the foundation of any lasting partnership.

Will Morey: Listening, acting, and celebrating

Following Marler's riotous close, Will Morey return to the stage to wrap up the day with characteristic warmth and clarity.

Summarising the event, he reinforced Gamma's dual commitments: to listen closely to partner feedback and to act decisively on it. "Listening only goes so far," he said. "We have to turn what we hear into something meaningful, products, services, and experiences that help you grow your business." He also announced the return of the Gamma Ball Rally in 2026, an event beloved in the channel for its mV of fun, fundraising, and friendly competition. "We want to make sure that every success we share with you is celebrated properly," Morey added.

A broader message

If Gammaverse 2025 had a unifying theme, it was that progress depends on partnership and courage. Partnership to stay aligned, and courage to keep evolving.

The event moved seamlessly between strategy, innovation, and storytelling, but what tied it together was the sense that Gamma's partners are not passengers on its journey. They are co-authors of its next chapter. Between Conniff's call to "rewrite the code," Marler's lessons in resilience, and Morey's focus on listening and action, the day left the audience with both inspiration and direction.

In a market shaped by consolidation, competition, and constant technological change, that clarity matters. As one attendee summed it up: "It's good to be reminded that collaboration and creativity can still win against scale." Gamma seems to agree. "We're more motivated than ever to drive on and support partner success," Morey concluded.

The final word

Gammaverse 2025 wasn't about selling or showcasing. It was about reminding the channel why it works: because it listens, learns, and leads together. Whether you came for the roadmap, the rule breaking, or the rugby stories, the message was the same. The future belongs to those who collaborate, experiment, and celebrate the wins along the way.

If that sounds a bit pirate, it's because it is.

There is plenty of follow up activity. Please visit gammagroup.co to speak to a team member.

if you missed the event or would like to watch it again, visit the post event page here: Gammaverse 2025 Post Event Page