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

COMPLIANCE CRUNCH

MSPS ARE PERFECTLY PLACED TO HELP SOLVE IT

MSP CHANNEL INSIGHTS

ROADSHOW 3

Utrecht, The Netherlands

Venue: Crowne Plaza Utrecht Central Station

6 November 2025

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

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

HEADLINE SPONSOR
Kaseya®

msp-roadshow.com

VIEWPOINT

BY PHIL ALSOP
EDITOR

MSP 3.0 and beyond: reinventing the channel for a secure, scalable, AI-driven future

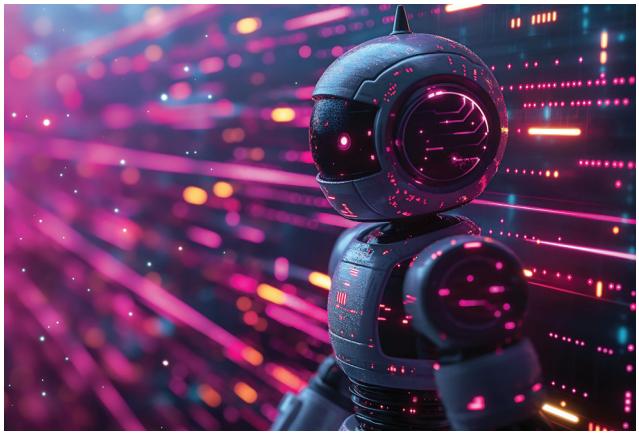
THE managed services market is undergoing a defining transformation. Once seen as backend support providers, today's MSPs are expected to be agile, strategic enablers - delivering not just technology but innovation, resilience, and regulatory peace of mind.

At the core of this evolution is cybersecurity. As threat actors increasingly target MSPs for their privileged access, the need for built-in, not bolt-on, cyber resilience has become urgent. CyberSmart's blueprint makes clear that effective security isn't about complexity it's about execution. Patching, MFA, backups, and user training remain simple but critical defences that too many providers still neglect.

In parallel, compliance is no longer a back-office concern. New mandates like NIS2 and DORA raise the bar for operational resilience, third-party visibility, and incident response. Trend Micro's view reframes compliance as an opportunity for MSPs to shift from vendor to trusted advisor helping clients manage cyber risk exposure proactively rather than reactively.

But evolving customer demands are rewriting the rulebook. UBDS highlights how younger, tech-native buyers expect DevOps-style engagement, rapid deployment, and outcomes, not hours billed. This shift is pushing MSPs to integrate AI and automation more deeply, even as adoption remains experimental. The real opportunity lies not in gimmicks but in practical applications like self-healing systems and service orchestration.

Meanwhile, multi-tenancy is quietly becoming the backbone of the modern MSP model. As Zadara explains, shared



infrastructure enables security, scalability, sustainability, and cost-efficiency. It's a win-win: customers enjoy enterprise-grade service without the enterprise overhead, while providers streamline delivery and improve margins.

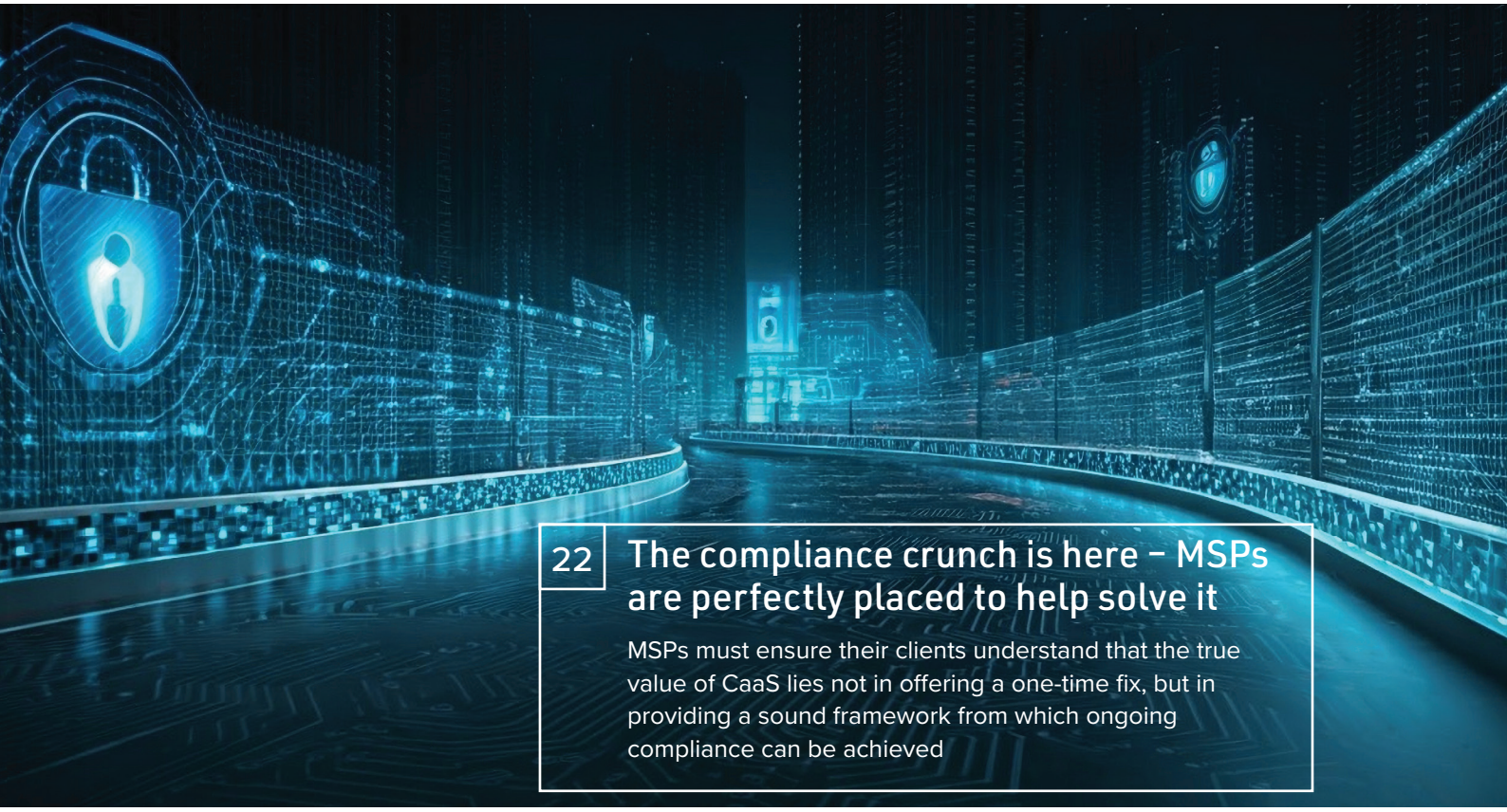
Finally, the infusion of AI into telecom and unified communications, as CallTower notes, is revolutionising customer engagement, analytics, and operational efficiency. But success will hinge on balancing technological capability with data ethics, workforce readiness, and customer trust.

In short, the MSP market is maturing. Those who embrace security-by-design, regulatory fluency, AI experimentation, and scalable architectures will lead the next chapter. MSP 3.0 isn't a prediction it's already here. The question is who's ready to meet its demands.

CONTENTS

ISSUE III 2025

MSP CHANNEL INSIGHTS



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 six 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)

97% of businesses to use AI in customer communications

New research from Sinch reveals how top brands are unlocking smarter, more personalized customer experiences with AI, RCS, and integrated omnichannel strategies.

SINCH has released new research indicating that nearly all businesses plan to incorporate artificial intelligence into their customer communications this year. The report, the state of customer communications, explores how brands are adapting their engagement strategies as customer expectations rise, and AI adoption accelerates globally.

Based on surveys of 2,800 consumers and 1,600 business leaders across industries including retail, financial services, healthcare, and technology, the report shows that AI is set to play a central role in transforming how companies build seamless omnichannel execution across channels and deliver real-time support and personalized experiences.

The findings show that consumers increasingly expect consistent, secure, personalized experiences across channels like SMS, email, chat, and voice. Businesses are responding by integrating their communication strategies to deliver more seamless, AI-driven omnichannel engagement.

“Customer communication is no longer just about sending a message. It’s about creating moments that engage people and drive business results,” said Gwen Lafage, VP of Brand and Content at Sinch. “The businesses that lead are putting the customer at the heart of their communication strategies, letting them choose how and where they want to connect and using AI, and channels like RCS, to make every interaction smarter, faster, and more meaningful. That is how you create standout experiences and real business impact.”

Key findings from the report:

- The research identifies key trends shaping the future of digital customer communications, where AI, trust, and omnichannel execution intersect to deliver better customer experiences.

- **AI adoption is accelerating**
  97% of businesses plan to use AI in their customer communications this year, with top investment areas for 2025 including AI voice assistants (63%) and AI-driven chatbots (43%). AI is quickly becoming the foundation of modern engagement strategies, providing real-time support, smarter personalization, and secure verification.
- **AI trust is generational**
  Millennials and Gen Z are embracing AI-powered interactions for speed and ease. In contrast, older consumers remain more cautious, particularly around transparency and data usage. 71% of Gen Z respondents would work with an AI-chatbot trained on support documentation. That compares to 42% of all age groups
- **Consumers expect channel choice and relevance**
  58% of consumers want to choose the channels they receive messages on, with preferences varying by use case and demographic. Businesses are under pressure to match these expectations with more flexible, personalized, and integrated communication strategies.
- **RCS is gaining traction**
  59% of business leaders view Rich Communication Services (RCS) as a game-changer. This mobile messaging option was also consistently chosen by consumers over other formats for promotional, informational, and verification messages. The channel includes features like verified sender, image carousels, video, quick replies, and embedded calls to action, transforming what’s possible in mobile messaging.

To help brands transform single interactions into real relationships, Sinch introduces a simple framework built around four essential use cases that drive both customer experience and business impact:

- **Marketing campaigns:** Keep customers engaged with personalized messages that capture attention and drive conversions.
- **Customer updates:** Keep customers informed with personalized alerts that drive timely actions and reduce operational inefficiencies.
- **Identity and verification:** Keep customers safe by securing identities and interactions and preventing fraud through verified communication.
- **Customer service:** Keep customers happy with fast, responsive support that builds loyalty and retention.

As competition intensifies and customer expectations continue to rise, the ability to deliver clear, secure, and relevant omnichannel communication is becoming a key business priority.
“It has never been more important, or more achievable, to create experiences that customers love,” said Sophie Cheng, SVP of Product Marketing at Sinch. “But to do that, businesses must embrace AI to create seamless, trusted omnichannel strategies that focus on keeping their audiences engaged, informed, safe, and happy. That’s exactly what our framework delivers: a clear focus on smarter digital communications that drive stronger business outcomes.”

SMBs are aware of cyber risks but slow to act

Cyber threats are accelerating, but many small and medium-sized businesses (SMBs) are stuck in neutral.

DESPITE increasing awareness and rising investment in cybersecurity, too few are making the leap from confidence to capability. In fact, 71% of SMBs say they feel confident in handling a major cybersecurity incident – yet only 22% report having an advanced cybersecurity posture, according to Devolutions' newly released report, "The State of IT Security for SMBs in 2025."

Based on input from 445 IT, security and executive professionals around the world, the report reveals that this gap between perception and reality is leaving many SMBs vulnerable – particularly in three key areas:

- **Privileged Access Management (PAM),** Artificial Intelligence (AI) adoption, and cybersecurity budgeting. Devolutions, a global leader in secure software solutions, conducted the study to help organizations better understand how they can bridge the divide between IT management and security – and where many are still falling short.

- **PAM: Still Manual, Still Risky**
  Despite its critical role in minimizing insider threats and credential abuse, 52% of SMBs still rely on manual tools – like spreadsheets or shared vaults – to manage privileged access. That number has grown since 2023.
- **AI: Everyone's Talking, Few Are Doing**
  From automated threat detection and anomaly spotting to predictive analysis and behavior-based access control, AI promises faster, smarter and more scalable defense.

However, as the survey points out, promise and practice are two very different things. 71% of SMBs plan to increase their use of AI in cybersecurity, but only 25% are using it today – and 40% haven't started at all. Concerns around cyberattacks on AI systems, data privacy, and skill gaps are slowing momentum.

"Artificial intelligence is a powerful advancement, but like fire, it must be handled with care," said Martin Lemay, CISO at Devolutions. "It's not without flaws, and its reliance on vast amounts of data makes strong governance and clear regulations essential to prevent misuse."

Budgets Are Up – But Misaligned
While 63% of SMBs increased their cybersecurity spending, nearly a third still allocate less than 5% of their IT budget to security. Many organizations are spending more – but not necessarily spending smarter, and too many organizations still underfund their security efforts relative to their risk exposure.

Data silos prevent healthcare organisations from capitalising on the AI opportunity

ONLY 54% of organisations have robust systems for moving data internally, while only 56% have accurate and consistent data.

Healthcare organisations believe AI will be vital to their operations, but lack the data processes and systems to capitalise on the opportunity, global research released by SS&C Blue Prism has revealed.

Surveying 297 senior professionals in the healthcare sector, the research found that 94% of organisations believe that AI is core to their entire operations. Executives believe improving care quality (42%), minimising repetitive and manual processes (36%) and enhancing patient experiences (34%) are the key areas in which AI can help in healthcare. With burnout still prevalent in healthcare systems globally, 37% of executives said staff believe that AI will help improve work/life balance for healthcare practitioners.

Agentic AI, the emerging technology where AI can make decisions and conduct activities autonomously, is a priority for the healthcare sector. Two thirds (67%) of organisations plan to implement agentic AI within 12 months. But the research shows that healthcare organisations need to get their data in order before making AI a reality. Only 54% of healthcare leaders said they have robust systems for moving data internally and only 56% say they have accurate and consistent data within their organisation. With data playing such an important role in delivering AI and personalising healthcare, the sector has work to do. Importantly, the healthcare sector topped all industries surveyed when it comes to data governance, with 72% saying they have strong governance systems in place to ensure data is secure, private and managed with the appropriate consents.

Focus on the individuals affected, not the number of breaches

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

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

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

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

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

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

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

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

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

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

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

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

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

"While it's unrealistic to expect organisations to prevent every breach, the data shows that implementing some basic controls could really make a difference," said Peter Woollacott, CEO at Huntsman Security. "Adhering to established security frameworks like NIST or the ACSC Essential Eight can dramatically reduce, not only the number of incidents, but – more importantly –the number of people affected by those incidents overall.

Putting in place baseline controls such as effective and timely patching, multi factor authentication, user application hardening and regular backups can make the world of difference when it comes to effective cyber security."
He added: "What's needed is better visibility through a shift from periodic reviews to a more frequent, 'business as usual', approach that routinely identifies threats from mitigation, reports control effectiveness and reassures both security and executive stakeholders. Annual assessments or audits are simply no longer enough to protect against data theft."

Organisations need immediate visibility into their security posture, with actionable insights that inform the risk mitigation team. Slow response times were highlighted in the Australian data and with cyber threats constantly evolving, tracking the state of security defences on a regular basis is now a priority. It is essential for protecting data, maintaining trust and avoiding costly disruption.

AI agents go mainstream

Over 80% of companies to use them within three years.

IN JUST two years, AI agents, autonomous systems that can work on their own, complete tasks from start to finish, and team up with other agents, have evolved from experimental tools into mainstream solutions.

Last year, even major enterprises like OpenAI, Google DeepMind, Microsoft, and PwC began integrating them into their operation, proving them as one of the top AI trends. Moreover, this is just the beginning of AI agents` growth, with market projections showing a surging adoption in the years ahead.

According to data presented by Techgaged.com, around 51% of organizations plan to partially or fully scale up AI agents in 2025, and this figure is projected to jump to 82% within the next three years.

From insurance and healthcare to aerospace and defense, 7 in 10 executives rank AI agents among the top 3 AI trends.

Just a few years ago, it was hard to imagine AI agents becoming mainstream. Today, they're key tools for businesses, helping them save time and work better by analyzing data, making strategic decisions, taking action, and talking to users in real time. This approach has completely changed how organizations work and grow their business, but it's just the start of a new surging trend.

According to the Capgemini Top Tech Trends of 2025 survey, 51% of companies plan to partially or fully scale up AI agents this year to boost efficiency and develop automation.

While this represents a significant leap compared to just two years ago, the adoption of AI agents will explode in the next three years, with an impressive 82% of companies set to adopt them fully or partially.

This projection aligns with how tech executives and investors rank AI agents among the top AI and tech trends. Statistics show that 70% of industry executives and 85% of investors focused on AI and data technologies named AI agents one of the three most impactful technologies in 2025.

Analyzed by sectors, AI agents` adoption is most likely to soar in the insurance and retail industries, where 85% and 81% of executives see them as the leading tech trend. Consumer products, energy and utilities, government and public services, and banking also show strong support, with between 70% and 75% of executives thinking the same. Even in sectors with slightly lower figures, including automotive, healthcare, high-tech, aerospace, and defense, around 60% of executives still view AI agents as a major trend.

AI Agent Market Value Set to Soar 821%, Reaching $47 Billion by 2030

With big tech companies ramping up innovation and investment in AI agents and pushing the limits of what AI can do, the market is set for explosive growth by the end of the decade. Last year, the AI agent industry was valued at around $5.1 billion. This figure is projected to soar by a whopping 821%, reaching $47 billion by 2030.

To put that into perspective, that is nearly twice the projected growth in the machine learning sector, the fastest-growing segment of the AI industry, almost six times the growth in the computer vision segment, and 2.7 times larger than the five-year growth forecast for both the AI robotics industry and the broader AI market.

A major infrastructure shift is underway

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

Combined with the ubiquity of connected devices, 24/7 uptime demands, and intensifying security threats, these shifts are driving infrastructure to adapt and evolve. The result: IT leaders are changing how they think about the network: what it is, what it enables, and how it protects the organization. The network they build today will decide the business they become tomorrow.

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

IT leaders are already delivering financial value from today's networks – largely by improving customer experiences (55%), boosting efficiency (52%), and enabling innovation (51%).

But much of that value is at risk if it comes from infrastructure that hasn't been designed for AI or real-time scale. To unlock the full growth and savings they expect, leaders have identified critical gaps they must close: siloed or partially integrated systems (58%), incomplete deployments (51%), and reliance on manual oversight (48%).

Smarter, more secure, more adaptive networks are the business case for investment. Nearly 9 in 10 (89%) say improved networks will directly drive revenue, and almost everyone (93%) expects meaningful cost savings – driven by smarter operations, fewer outages, and lower energy use.

97% of mid-market organisations intend to migrate applications or workloads from the public cloud

Data from 'Unlocking Growth in the Mid-Market: The Node4 Report', reveals UK mid-market leaders are taking a more pragmatic approach to public cloud consumption.

NEW INDEPENDENT research commissioned by Node4 reveals 97% of mid-market companies plan to migrate some workloads out of their public cloud environments over the next 12 months. However, far from signalling the end of public cloud, this trend reflects a more targeted and pragmatic approach, where organisations optimise location and workload in environments that work best for their specific needs. In this context, it's notable that only 5% intend to repatriate all their applications.

The majority (49%) plan to remove a few specific applications and workloads. "Mid-market organisations are entering a new phase of cloud strategy – one defined by pragmatism, not dogma," comments Richard Moseley, CEO, Node4. "Most still have a substantial footprint of on-premises infrastructure and applications running in the public cloud. This demonstrates a clear preference for hybrid environments and a shift from cloud-first to cloud-appropriate. We believe this will be the mid-market's default setting for the foreseeable future."

According to 'Unlocking Growth in the Mid-Market: The Node4 Report', performance considerations top the list of reasons for migrating selected applications away from public cloud environments—and are due to:

- Lift and shift workloads that were unsuited to the public cloud
- Applications that have been modernised but aren't performing as expected
- User frustrations from SaaS application latency

"Organisations that migrated to the public cloud several years ago have realised that while their environments provide many benefits and offer more scalable on-demand performance

than other hosting options, they aren't always the best fit for every application.

This applies particularly to organisations that lifted and shifted to the public cloud without due planning and strategy – perhaps with legacy systems or databases that were never intended for cloud consumption," explains Richard Moseley.

Mid-market business leaders cited data sovereignty (30%) as the second most likely reason to repatriate workloads from public cloud environments. While concerns around regulations like DORA, GDPR and the US Cloud Act are part of this picture, this result reflects a broader unease about control, jurisdiction, and long-term data access—especially for those in regulated or compliance-heavy environments.

Other reasons for repatriation include risk management (29%), technical limitations (27%), cost optimisation (26%), compliance (26%), and security (21%). Looking at security in particular, data suggests that respondents who run primarily on-premises infrastructure are more confident in preventing and responding to cyberattacks than those with fully cloud-based infrastructure.

This is a counterintuitive result as most mid-market organisations would struggle to replicate the advanced security and access configurations available in public cloud environments.

Commentary from within the research highlights several reasons, including a perceived loss of control, complexity, limited visibility and skills gaps—all of which impact the ability of mid-market organisations to take full advantage of cybersecurity protection in public cloud environments.

Richard Mosely concludes: "Public cloud still plays a vital role for the mid-market, but it's no longer the default. Our data shows mid-market leaders are optimising for performance, compliance, and more direct control. Businesses that get this balance right will unlock greater efficiency, agility, and resilience from their infrastructure investments. This, in turn, will lay the foundations for improved growth and productivity."

Short-term thinking and delayed investment in technology are stopping CIOs in their tracks

According to research unveiled today, one in five CIOs and CTOs at enterprise companies (21%) believe that their organisations' road to digital transformation has been hit by a focus on short-term results over long-term strategy.

WHEN ASKED what drives this short-term thinking, nearly half (44.8%) said the main culprit was delayed investment in technology initiatives, while 40.6% blamed the pressure to demonstrate ROI.

The study, carried out by technology consultancy Crosstide, canvassed 500 CIOs and CTOs across the retail, asset & wealth management, insurance, life sciences, and payments industries, at UK-based companies with £750m+ annual revenue.

It revealed that to improve their organisation's ongoing digital transformation journey (aside from asking for more budget), CIOs and CTOs at enterprise companies also need:

- More empowerment to affect real change (according to 23.4% of CIOs/CTOs)
- More investment in AI (22.8%)
- Stronger cyber-security (21.2%)
- Clearer direction from the CEO/board (20.8% - rising to 24.0% and ranked top among CIOs/CTOs at organisations that are more advanced in their digital transformation journey).

The study also asked CIOs/CTOs what is currently making it challenging to fulfil their role as a leader internally in their organisation's digital transformation journey.

The top challenge identified was legacy IT systems slowing progress (26.8%), followed by the poor perception of previous transformation projects and their impact on the business, and an inability to properly prioritise what should be tackled first (both 25.6%). The latter two challenges were even more pronounced in organisations that were more advanced in their digital transformation journey.

Richard Neish, CEO of Crosstide, said:

"It has never been harder to be an enterprise CTO or CIO.

"Challenging economic and sociopolitical pressures are slowing the pace of technology transformation. Investments in critical technology initiatives are being delayed, long-term roadmaps are giving way to short-term priorities, and technology leaders lack the direction, funding and empowerment to drive the change agendas demanded of them.

"Enterprise technology leaders find themselves squarely in the middle of competing priorities, unproven technologies, financial sensitivity and the pressure to deliver on rising expectations with falling budgets. "Good leaders are adopting new strategies to effect change, such as a test and learn mindset, building scalable foundations, measuring what matters and innovating how you work, not just what you build."

94% of organisations consider next generation AI core to their entire business operations

FINANCIAL SERVICES organisations see AI as the key to increase competitiveness and improve customer experience, but face barriers around data management and skills, research released today by SS&C Blue Prism has revealed.

Surveying 377 business leaders in the financial services sector, the research found that 94% of organisations believe that innovative AI is core to their entire business operations. The adoption of AI has been rapid in the financial services sector, with 87% actively deploying new AI technologies. Agentic AI, the emerging technology where AI can make decisions and conduct activities autonomously, is a high priority for the financial services sector. Three quarters (76%) of organizations surveyed plan to implement agentic AI within 12 months, but challenges remain.

Despite rapid adoption of AI throughout financial services, 38% said they do not have accurate and consistent data in their organisation and 37% do not have robust and efficient ways of moving data within their organisation. Breaking down data silos within an organization and creating consistent and accurate data is a major barrier to successfully deploy next generation AI.

Additionally, 31% of organisations admitted they don't have strong governance in place to make sure data is secure, private, and managed with the appropriate consents.

Data is not the only barrier to next generation AI success for financial organizations, finding the right skills and adopting to a more dynamic approach to innovation represent significant challenges. More than a third (36%) of financial services organisations say they lack the appropriate skills or technical expertise, 35% are concerned about extensive changes around employee training and management, and 33% are facing hurdles with technical integrations.

Why most businesses aren't yet winning with AI

71% of business leaders say their workforces are not ready to successfully leverage AI.

A NEW GLOBAL study released by Kyndryl finds that only a small number of organisations have taken steps to align their workforce strategies with the growth of AI technology.

Those that have done so have positioned themselves ahead in the race to deliver positive return on investments in the technology.

Based on a survey of more than 1,000 senior business and technology executives across 25 industries and eight geographies, Kyndryl's first People Readiness Report reveals a striking gap between AI investment and workforce preparedness:

- 95% of businesses have invested in AI
- 71% of leaders say their workforces are not yet ready to successfully leverage the technology
- 51% believe their organisations lack the skilled talent needed to manage AI
- 45% of CEOs think most employees are resistant or even openly hostile to AI Workforce readiness varies by industry.

Businesses in Banking/Financial Services and Insurance report the highest levels of preparedness, while those in Healthcare report trailing behind.

"Only a small group of businesses have been able to harness AI successfully for business growth," said Michael Bradshaw, Global Practice Leader for Applications, Data and AI. "This report shows that while data architecture and technology infrastructure are key pieces of the puzzle, organisations that do not prioritise their workforces and organisations will miss out."

Despite widespread attempts at implementation, most organisations are not currently benefiting from game-changing use cases that will drive new products and services for their

customers. Generative AI tools are the most popular use case reported by those surveyed, yet only 4 in 10 leaders report using AI-powered insights to enhance decision-making or unlock growth for their business. Just one-fifth of leaders say the primary use case of AI at their organisation is to develop new products and services for customers.

Yet this research also reveals that a small subset of AI Pacesetters has leveraged AI for business growth while addressing workforce readiness. They are making strategic workforce decisions and seeing benefits across their employee population. Pacesetters are uniquely addressing 3 key barriers that are inhibiting AI adoption, and they are seeing benefits from their actions across:

- **Organisational change management:** AI Pacesetters are three times more likely than others to report a fully implemented change management strategy for AI in the workplace.
- **Lack of employee trust in AI:** AI Pacesetters are 29% less likely to cite fears around AI affecting employee engagement.
- **Skill gaps:** AI Pacesetters are 67% more likely to agree that their organisation has the tools and processes to accurately inventory the skills employees currently have. Four in 10 report no skills challenges at all.

"Preparing your workforce for the era of AI is easy to say, hard to do and an urgent imperative for business leaders," said Maryjo Charbonnier, Chief Human Resources Officer at Kyndryl. "At Kyndryl, we run an entire ecosystem of systems and culture that readies our people and our business for continuous change. It's about anticipating the business impacts of AI, understanding and integrating your skill data with your customer demand and having a multi-pronged approach for equipping employees to build the skills they need and learn to effectively use generative AI tools in their work."

Compared to CIOs and CTOs, CEOs are far more likely to say their organisation is still in its early stages of AI, and two and a half times more likely to say their infrastructure is inadequate to support it. This difference also extends to how they choose to solve AI-related workforce challenges and the individual skills they believe their organisation needs to be successful. CEOs are far more likely to turn to outside talent rather than upskilling their own employees

MSP CHANNEL AWARDS 2025

CELEBRATING 15 YEARS OF SUCCESS

WE'RE PROUD TO HAVE LAUNCHED THE MSP CHANNEL AWARDS

INTRODUCING THE MSP CHANNEL AWARDS

A refreshed and rebranded evolution of the highly respected SDC Awards. This transformation reflects the growing influence of Managed Service Providers, who are now leading the way in delivering cutting-edge IT solutions across every industry.

We still have categories covering storage, backup, cybersecurity, and cloud infrastructure but we have added exciting new categories to better reflect the modern MSP ecosystem and the broader channel community — including vendors, distributors, resellers, and integrators.

Getting involved is easy and completely free. You can submit as many products or projects as you like — this is your opportunity to highlight your innovation, showcase your successes, and gain industry-wide recognition.

NOMINATIONS ARE NOW OPEN

KEY DATES:

5 SEPTEMBER	NOMINATIONS CLOSE
3 OCTOBER	SHORTLIST ANNOUNCED
6 OCTOBER	VOTING OPEN
7 NOVEMBER	VOTING CLOSES*
3 DECEMBER	AWARDS CEREWMONY

* Voting will close 17:30 GMT

Winners will be announced at a gala evening on 3 December 2025 at Leonardo Royal Hotel London City, London.

NOMINATE NOW!

mspchannelawards.com

T: +44(0)2476 718 970

Angel BUSINESS COMMUNICATIONS

SDC AWARDS

ANGEL EVENTS

Global cloud infrastructure spending rose 21% in Q1 2025

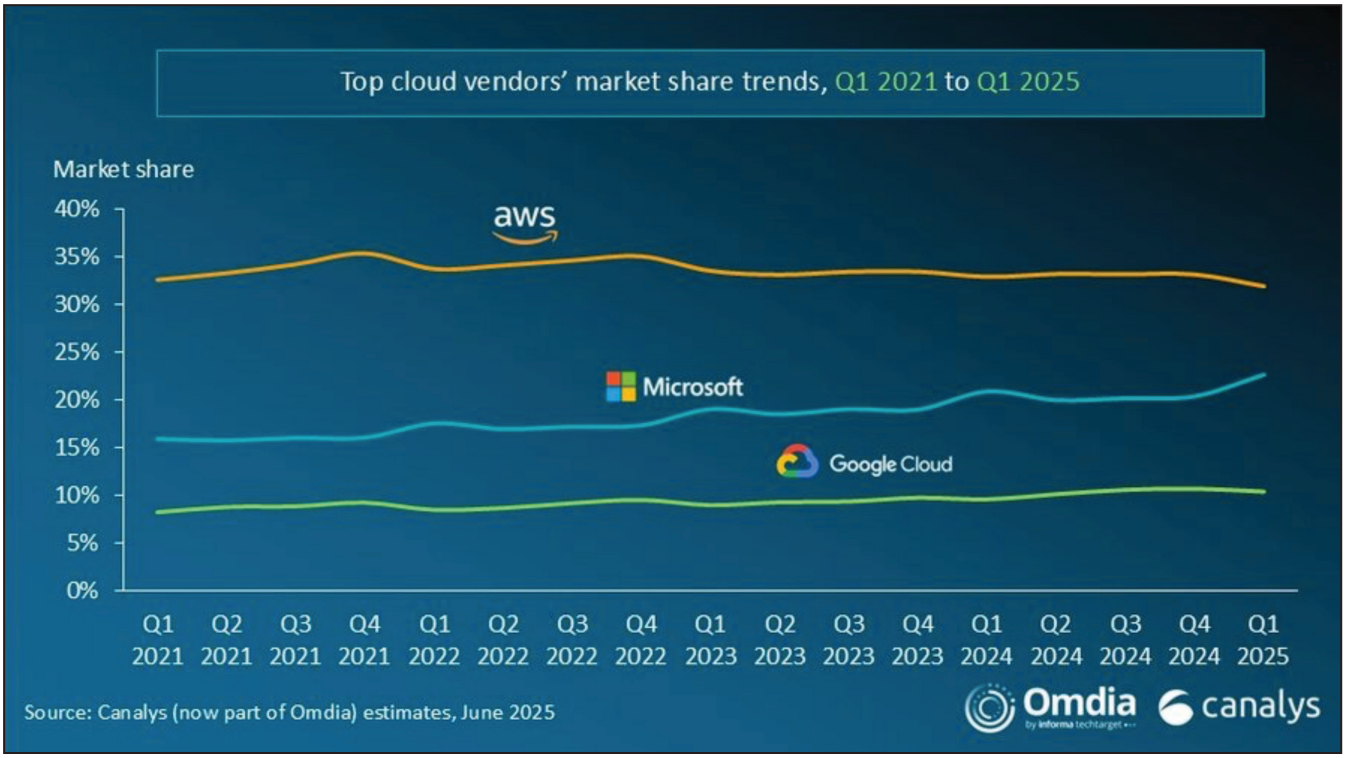
Global spending on cloud infrastructure services, according to Canalys (now part of Omdia) estimates, reached US$90.9 billion in Q1 2025, marking a 21% year-on-year increase.

ENTERPRISES have recognized that deploying AI applications requires renewed emphasis on cloud migration. Large-scale investment in both cloud and AI infrastructure remains a defining theme of the market in 2025.

Meanwhile, to accelerate the enterprise adoption of AI at scale, leading cloud providers are intensifying efforts to optimize infrastructure – most notably through the development of proprietary chips—aimed at lowering the cost of AI usage and improving inference efficiency. In Q1 2025, the ranking of the top three cloud providers (AWS, Microsoft Azure, and Google Cloud) remained unchanged from the previous quarter, with their combined market share accounting for 65% of global cloud spending. Collectively, the three hyperscalers recorded a 24% year-on-year increase in cloud-related spending.

Growth momentum diverged among the top players. Microsoft Azure and Google Cloud both maintained growth rates of over 30% (although Google Cloud's growth slowed slightly from the previous quarter), while AWS grew by 17%, a deceleration from 19% growth in Q4 2024. This deceleration was largely driven by supply-side constraints, which limited the ability to meet rapidly rising AI-related demand. In response, cloud hyperscalers have continued to invest aggressively in AI infrastructure to expand capacity and position themselves for long-term growth.

Overall, the global cloud services market sustained steady growth in Q1 2025, as enterprises sharpened their focus on two strategic priorities: accelerating cloud migration – either by shifting additional workloads or reviving stalled on-premises transitions – and exploring the adoption of generative AI.



The rise of generative AI, which relies heavily on cloud infrastructure, has in turn reinforced enterprise cloud strategies and hastened migration timelines.

"As AI transitions from research to large-scale deployment, enterprises are increasingly focused on the cost-efficiency of inference, comparing models, cloud platforms, and hardware architectures such as GPUs versus custom accelerators," said Rachel Brindley, Senior Director at Canalys (now part of Omdia).

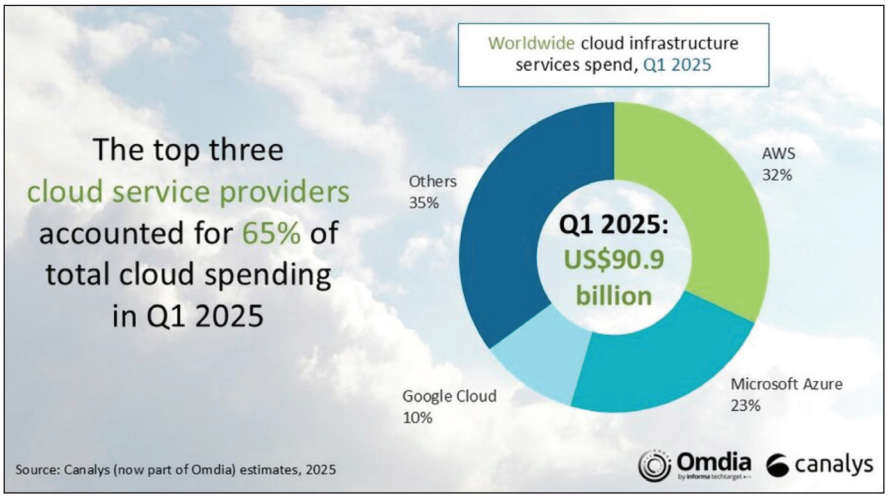
"Unlike training, which is a one-time investment, inference represents a recurring operational cost, making it a critical constraint on the path to AI commercialization."

"Many AI services today follow usage-based pricing models—typically charging by token or API call—which makes cost forecasting increasingly difficult as usage scales," added Yi Zhang, Analyst at Canalys (now part of Omdia). "When inference costs are volatile or excessively high, enterprises are forced to restrict usage, reduce model complexity, or limit deployment to high-value scenarios. As a result, the broader potential of AI remains underutilized."

To address these challenges, leading cloud providers are deepening their investments in AI-optimized infrastructure. Hyperscalers including AWS, Azure, and Google Cloud have introduced proprietary chips such as Trainium and TPU, and purpose-built instance families, all aimed at improving inference efficiency and reducing total cost of AI.

Amazon web services (AWS) maintained its position as the market leader in Q1 2025, capturing 32% of global market share and recording a 17% year-over-year increase in revenue. Its AI business continues to grow at a triple-digit annual rate, though it remains in the early stages of development.

In March, AWS introduced a price-cutting strategy to promote adoption of its Trainium AI chips over more costly NVIDIA-based solutions, highlighting Trainium 2's 30–40% price-performance advantage. The company also accelerated the expansion of its Bedrock service, adding Anthropic's



Claude 3.7 Sonnet and Meta's Llama 4 models, and became the first cloud provider to fully manage DeepSeek R1 and Mistral's Mixtral Large.

Further underscoring its long-term commitment to global infrastructure, AWS announced a capital investment of over US$4 billion in May 2025 to establish a new cloud region in Chile by the end of 2026.

Microsoft Azure remained the second-largest cloud provider in Q1 2025, holding a 23% market share and delivering strong year-over-year growth of 33%. Microsoft reported a 16 point growth rate lift to Azure from AI, marking the largest single-quarter uplift since Q2 2024.

In April, Azure announced the availability of the GPT-4.1 model series on both Azure AI Foundry and GitHub, further broadening developer access to advanced AI capabilities across its ecosystem.

Azure AI Foundry, Microsoft's platform for building and managing AI applications and agents, is now used by developers at more than 70,000 enterprises.

The platform processed over 100 trillion tokens this quarter, a fivefold increase year-over-year. Microsoft has also focused on lowering the cost of AI adoption, reporting a nearly 30% improvement in its AI performance at constant power consumption and a reduction of over 50% in cost per token. As part of its ongoing global infrastructure expansion, it opened new data centers in 10 countries across four continents during Q1.

Google Cloud, the world's third-largest cloud provider, maintained a 10% market share in Q1 2025 and delivered strong year-over-year growth of 31%. As of 31 March, its revenue backlog reached US$92.4 billion, marking a slight decline from the previous quarter.

This decrease was primarily attributed to supply constraints, particularly in compute capacity, that limited Google Cloud's ability to fully meet customer demand. In March, Google introduced the Gemini 2.5 model series, with Gemini 2.5 Pro receiving widespread acclaim for its leading benchmark performance and top ranking on Chatbot Arena.

With enhanced reasoning and coding capabilities, the model opens new possibilities for both developers and enterprise users.

Since the beginning of the year, active usage of Google AI Studio and the Gemini API has surged by over 200%, reflecting strong developer adoption and growing demand for generative AI solutions.

Google also launched a new cloud region in Sweden (its 42nd globally) and committed US$7 billion to expand its Iowa data center, further supporting its growing AI and cloud workloads.

Canalys (now part of Omdia) defines cloud infrastructure services as the sum of bare-metal-as-a-service (BMaaS), infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and container-as-a-service (CaaS) and serverless that are hosted by third-party providers and made available to users via the Internet.

Areas for CISOs to harness hype and drive meaningful change

Chief information security officers (CISOs) must focus on three areas to harness increased hype and scrutiny and turn disruption into opportunity, according to Gartner, Inc. These three areas include being mission-aligned, innovation-ready and change-agile.

"ORGANIZATIONS are making aggressive technology investments to achieve their goals, especially in leading edge, 'hyped' areas like GenAI," said Katell Thielemann, Distinguished VP Analyst at Gartner. "Leaders aren't just placing bets on GenAI and other explorative technology; they're also concerned about the cybersecurity risks associated with them."

"Cyber incidents associated with explorative technology are now hitting the bottom line, so executives are paying attention to cybersecurity," said Leigh McMullen, Distinguished VP Analyst and Gartner Fellow. "Becoming students of hype can really help CISOs further their own agendas under this scrutiny."

During the opening keynote of the Gartner Security & Risk Management Summit, Thielemann and McMullen outlined three key areas to help anticipate the future needs of CISOs and allow them meet the needs of today's complex, fast and unpredictable reality.

Be mission-aligned

CISOs must prove that their cybersecurity efforts are aligned to their organization's mission by transparently showing how cyber investment decisions and exposure implications should work together. "When change ambitions are at their peak, CISOs need to ground people in reality and data," said Thielemann. To achieve this, CISOs must start by identifying outcome-driven metrics (ODMs), or metrics that measure the current level of cybersecurity protection and exposure.

"ODMs allow CISOs to communicate transparently and agree on protection levels with the enterprise," said McMullen. "They are a way to express current exposure levels and drive a conversation with stakeholders about their desired targets, whether it is the board, CEO, CIO or anyone else."

Once the ODMs are set, CISOs must next explore protection level agreements (PLAs), which can be used to enable mission-aligned transparency. PLAs are a formal agreement on the amount of money the enterprise is willing to spend to deliver a desired level of cybersecurity protection.

"When CISOs communicate in terms of protection levels and buying down exposure levels, they are less likely to get caught up in someone else's marketing hype," said McMullen. "This eventually helps CISOs prove that their cybersecurity efforts are aligned to their organization's mission."

Be innovation-ready

CISOs should be innovating with AI in cybersecurity, which ultimately will help an organization's overall longer-term AI ambitions. "Cybersecurity should be the place where many enterprises start experimenting and finding real value from AI," said McMullen.
CISOs should explore three steps to enable their organization's longer-term AI ambitions:

- Cultivate AI literacy for themselves and their teams.
- Experiment with AI in cybersecurity, from code analysis, to threat hunting

and modeling, to user behavior analysis.
- Protect AI investments in their organizations by taking actions such as revising data retention policies to protect prompts, input, and output storage; implementing comprehensive risk assessments for custom-built GenAI; and carrying out regulatory compliance audits.

Organizations should clearly define AI's role, prioritize strategic objectives, and determine the roles of human agents. This strategic alignment is essential to enhance customer service without compromising quality, ensuring that AI serves as a complement rather than a replacement for human interaction

Being change-agile

CISOs uniquely know that AI brings more security risks and that AI-assisted insider threats and attack surface will increase.

"The combination of effects are dizzying, so it pays to be a student of hype when it comes to change," said Thielemann. "Organizational change is both powered and limited by hype. If CISOs understand how hype flows, they can use its energy to our advantage. "One way to harness the hype is by 'Taking a Distanced View of Close Things,'" continued Thielemann. "As a CISO, you may see 1,000 conflicting initiatives piling up on your desk coming at you from everywhere out of corporate desperation. As a student of hype you can read the change energy and anticipate the ebbs and flows on your teams and business partners."

In an era where employees are increasingly change resistant and even fearful of AI, CISOs must be on the lookout for burnout from their employees, whether that is through unexpected surprises, a feeling of lack of agency or via boring, repetitive tasks. "CISOS must be able to empower their teams to be part of the solution and feel agency," said McMullen. "If CISOs' teams feel agency, they will want to focus on automating repetitive tasks and developing new skills to fuel your growth as well as theirs, which in turn will make them resilient agents of change no matter what that change is."

50% of organisations will abandon plans to reduce customer service workforce due to AI

By 2027, 50% of organizations that expected to significantly reduce their customer service workforce will abandon these plans, according to Gartner, Inc. This shift comes as many companies struggle to achieve their "agent-less" staffing goals, highlighting the complexities and challenges of transitioning to AI-driven customer service models.

A Gartner poll of 163 customer service and support leaders conducted in March 2025 found 95% of customer service leaders plan to retain human agents to strategically define AI's role. This approach ensures a "digital first, but not digital only" strategy, avoiding the pitfalls of a hasty transition to an agentless model.

"While AI offers significant potential to transform customer service, it is not a panacea. The human touch remains irreplaceable in many interactions, and organizations must balance technology with human empathy and understanding," said Kathy Ross, Senior Director Analyst in the Gartner Customer Service & Support practice. "A hybrid approach, where AI and human agents work in tandem, is the most effective strategy for delivering exceptional customer experiences." Organizations should clearly define AI's role, prioritize strategic objectives, and determine the roles of human agents. This strategic alignment is essential to enhance customer service without compromising quality, ensuring that AI serves as a complement rather than a replacement for human interaction. As the landscape of customer service continues to evolve, integrating AI with human capabilities is essential. This will not only improve service quality but also ensure that organizations remain agile and responsive to customer needs.

Worldwide UC&C revenues grew 7.8% YoY in 2024

i n 2024, the worldwide Unified Communications & Collaboration (UC&C) market revenues grew 7.8% year over year (YoY) to $69.2 billion, according to the International Data Corporation's (IDC) Worldwide Quarterly Unified Communications and Collaboration Tracker. Further, the worldwide UC&C market is forecast to grow at a compounded annual growth rate (CAGR) of approximately 3.9% during 2025-2029 to reach cumulative revenues of $85.4 billion.

INTEGRATED unified communications (UC) and customer engagement (CE) solutions represent the fastest-growing yet smallest segment in the global UC&C market. These solutions offer essential customer communications features and cater to organizations that need frequent customer interactions across functional teams but do not require a full-service contact center. This integrated UC-CE segment is a relatively recent market development and is expected to grow at a 33% CAGR from 2025 to 2029, reaching nearly $2 billion by 2029.

"The worldwide UC&C market is undergoing a massive transformation with new AI capabilities being released every quarter," said Denise Lund, Research VP, Worldwide Telecom and Unified Communications and Collaboration at IDC. "Businesses are recognizing the value of AI in UC Employee Engagement and UC Customer Engagement solutions. However, the AI-driven growth anticipated in the coming years will be counterbalanced by declines in IP Phones, IP PBX/ UC Systems, private cloud UCaaS, and videoconferencing infrastructure segments."

Meanwhile, worldwide revenues in the Communications Platform as a Service (CPaaS) market grew 7.7% YoY to $16.7 billion in 2024. "The worldwide CPaaS market is growing steadily as the demand for API-powered customized communications use cases continues to rise, particularly to leverage AI-driven capabilities," said Courtney Munroe, research vice president, Worldwide Telecommunications Research at IDC. During 2025-2029, CPaaS revenues are expected to grow at a 9.3% CAGR to $25.9 billion.

UC&C Company Highlights

- Microsoft's UC&C revenues rose 14% YoY to $31.5 billion in 2024, accounting for a 45.6% share of the worldwide UC&C market (up 2.4 percentage points from 2023).
- Zoom's UC&C revenue grew approximately 1% YoY in 2024 to $4.3 billion. The company accounted for a 6.2% market share, losing 40 basis points compared to 2023.
- Cisco's UC&C revenue fell 4.6% YoY to $3.7 billion in 2024, while its market share declined by 70 basis points YoY to 5.3% in 2024.

CPaaS Company Highlights

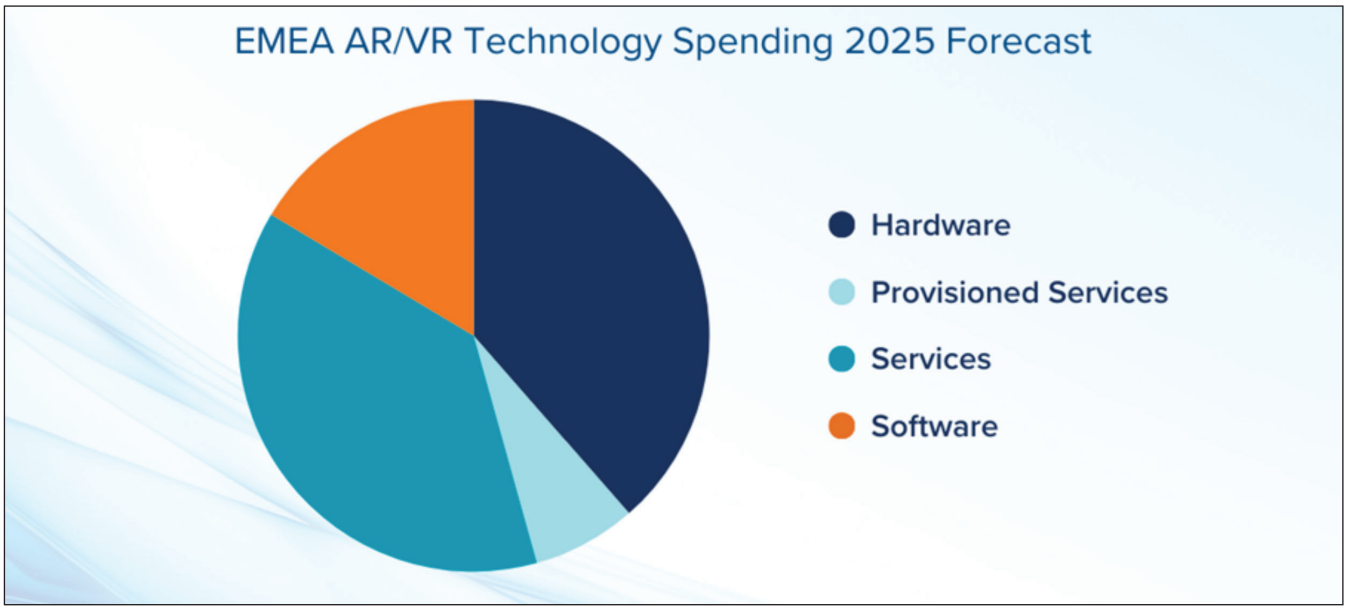
- Twilio continued to lead the worldwide CPaaS market with a 24% market share, up 70 basis points from 2023. Its CPaaS revenues surpassed $4 billion in 2024, growing 11% YoY.
- Sinch also maintained its second place with a 15% market share in 2024, down 1 percentage point from 2023. Its CPaaS revenue grew approximately 1% YoY to $2.4 billion in 2024.

EMEA's AR/VR spending to reach $8.4 billion by 2029

According to the Worldwide Augmented and Virtual Reality Spending Guide published by International Data Corporation (IDC), EMEA augmented reality (AR) and virtual reality (VR) spending will reach $8.4 billion by 2029, reflecting 16% five-year compound annual growth rate (CAGR). The consumer sector will lead investment in the AR/VR market, and this trend is expected to persist throughout the forecast period. However, enterprise adoption is also anticipated to rise due to the growing demand for headsets.

"The AR/VR market in the EMEA region is still in its early stages and remains sensitive due to economic volatility, which slightly hampers broader adoption," says Alexandra Rotaru, Data & Analytics manager at IDC Data and Analytics, Europe. "However, in the short to mid-term, growth in the AR/ VR market is expected to be driven by investments in mixed reality solutions to enhance remote collaboration, training activities, and immersive experiences in sectors like engineering, healthcare, manufacturing, and retail."

Industries such as engineering, healthcare, manufacturing, and retail are poised to lead the way in spending on AR/VR solutions, accounting for over half of the market by 2025. Engineering, construction, and real estate are using AR/VR to boost productivity, collaboration, and customer experiences through enhanced visualizations and improved training capabilities. In healthcare, AR/ VR is enhancing diagnostics and patient empowerment, while manufacturers are investing in these technologies to streamline operations and improve product quality. Consumers will continue to be the biggest spenders,



Source: IDC's Worldwide Augmented and Virtual Reality Spending Guide, V1 2025 (April), EMEA View

largely due to investments in the AR/VR-fueled gaming solutions.
As the market transitioned to include two new hardware categories, such as Mixed Reality (MR) and Extended Reality (ER) headsets, IDC estimates that MR headsets will contribute the most towards the overall hardware spending in EMEA.

According to the IDC's Worldwide AR/VR Headset Tracker, the linked product with the above-mentioned spending guide, MR headset volumes are expected to rise steadily due to higher customer demand, new models from Meta and Apple and the entry of new vendors in the market. IDC also predicts that the VR headsets will cease shipping by mid-2025 as the vendors will transition their products to mixed reality (MR) or extended reality (ER) headsets. "Meta remains the undisputed leader in the category, but competition is gaining momentum," says Diogo Santos, Data & Analytics analyst at IDC Data and Analytics, Europe. "In 2024, Meta accounted for three-quarters of the EMEA AR/VR market."

"However, new brands focusing on Extended Reality (ER), such as Even Realities and Xreal, are entering the scene. These products are increasingly appealing to consumers due to their design, portability, and innovative use cases. Although these brands currently ship relatively small volumes compared to Meta, their growth rate is extraordinary. Any stakeholder in this market should pay close attention to these rising stars."

When it comes to technology spending, the hardware category, including the headsets, remains a significant component of the AR/VR market in EMEA, while the software and provisioned services segments are experiencing the fastest growth, propelled by the development of MR applications, social VR platforms, and AR cloud technologies that facilitate shared digital experiences in physical spaces.

In terms of regional spending, Western Europe remains the largest market in terms of spending, while Middle East and Africa presents the fastest growing demand, with more than 20% five-year CAGR.

Why compliance is the next big opportunity for IT channel partners

As compliance regulations continue to evolve, channel partners must proactively adapt their strategies to meet new requirements while leveraging these changes as opportunities for differentiation.

BY BRIAN DAVIS, VP UK AND IRELAND, CLIMB CHANNEL SOLUTIONS

IF COMPLIANCE feels overwhelming right now, you're not imagining it. New regulations covering cybersecurity, data protection, AI, and more are emerging – from the latest PCI DSS updates to the EU AI Act. As a result, compliance is actively shaping the IT channel, influencing how we do business, how we anticipate industry shifts, and how we support our partners and customers with the right solutions to stay ahead.

Navigating compliance in 2025 means staying aligned with regulatory requirements, but it's a balancing act, because at the end of the day we all still have a job to do: delivering the right solutions, tailoring services to customer needs, and being a trusted partner in the channel.

With new regulations coming into force and the mounting challenge of understanding cybersecurity, AI governance, and data integrity requirements, it's more important than ever to stay ahead. Let's explore the key compliance trends of 2025: how partners can stay agile, deliver solutions that meet regulatory demands, and turn compliance into a competitive advantage

The agility advantage of smaller partners

Smaller channel partners face growing pressure from complex customer environments, resource constraints, and fierce competition for skilled talent. However, their agility provides a unique advantage. Unlike larger enterprises, they can quickly adapt to evolving customer needs, position themselves as trusted advisors, and identify emerging vendors—particularly those offering AI-powered and automated solutions. This flexibility positions them well to meet compliance and security challenges.

AI adoption plays a critical role in maintaining a competitive edge. By embracing AI, smaller partners can deliver exceptional managed services with fewer resources, keeping costs low and service quality high. This approach ensures they remain competitive in a crowded market.

Tackling the EU NIS2 directive

The EU NIS2 Directive reinforces the need for robust cybersecurity measures, urging businesses to adopt a more comprehensive approach to risk management. Essential security practices such as multi-factor authentication, regular cybersecurity training, incident response planning, and strong supply chain security are no longer optional but essential.

A key principle underlying the directive is the Identify, Detect, Protect, Respond, and Recover framework. While most organisations focus heavily on detection and protection, recovery is sometimes a weak link. A lengthy

recovery period following a breach can be as harmful as failing to detect the threat in the first place. The integration of automation into threat detection and response processes is becoming more important for meeting compliance requirements.

The EU AI Act: Compliance meets innovation

The EU AI Act introduces new obligations for organisations deploying AI solutions, emphasising transparency, accountability, and risk management throughout the AI lifecycle. These requirements extend to all aspects of AI implementation, from data sourcing and model training to real-world deployment.

To address compliance risks, managed service providers may consider introducing AI governance roles, such as "AI Managers as a Service." These specialists help organisations navigate AI regulations without requiring full-time in-house expertise.

While compliance with AI regulations may introduce additional costs, the long-term benefits—such as enhanced customer trust, clear documentation, and ethical AI practices—can significantly outweigh the initial investment. Rather than viewing compliance as a regulatory burden, partners should position it as an opportunity to strengthen customer relationships and stand out in the market.

Automation and AI: Key enablers of compliance

AI and automation are proving indispensable for managing compliance complexity. From automating repetitive processes to monitoring security events and ensuring adherence to evolving standards, these technologies help organisations streamline compliance efforts while minimising human error.

A practical starting point for partners is experimenting with AI-driven automation in their own operations. Deploying custom AI models for routine tasks can enhance efficiency and demonstrate real-world use cases to customers. Additionally, as security threats become increasingly sophisticated—driven by AI-powered cyberattacks—manual security interventions alone will no longer suffice.

AI and automation are proving indispensable for managing compliance complexity. From automating repetitive processes to monitoring security events and ensuring adherence to evolving standards, these technologies help organisations streamline compliance efforts while minimising human error

Emerging regulations and the importance of proactivity

Beyond the EU NIS2 Directive and AI Act, upcoming regulations such as the EU Cyber Resilience Act and the latest iteration of PCI DSS (v4) will further impact global compliance strategies. To stay ahead, partners must establish sustainable compliance programs that adapt to evolving regulations. Key actions include assigning ownership of compliance initiatives, continuously monitoring third-party providers, and refining policies to align with new regulatory requirements.

For PCI DSS compliance specifically, best practices include developing clear security policies, establishing performance metrics, and maintaining ongoing security awareness through continuous monitoring and regular testing. These principles can serve as a strong foundation for broader regulatory adherence, too.

Turning compliance into a market advantage

While regulatory compliance may appear daunting, it also presents a significant market opportunity. Forward-thinking channel partners can leverage compliance frameworks as a differentiator, demonstrating transparency and expertise to customers. Establishing internal AI evaluation teams can enhance both operational efficiency and credibility, positioning the business to meet evolving customer expectations. Innovation is as important as ever when it comes to compliance. Many organisations continue to rely on legacy systems to address compliance challenges, but evaluating emerging vendors and solutions is essential to staying ahead. As AI continues to transform the IT channel, partners that proactively adopt new technologies and regulatory strategies will be well positioned for success.

As compliance regulations continue to evolve, channel partners must proactively adapt their strategies to meet new requirements while leveraging these changes as opportunities for differentiation. Those who invest in AI, automation, and thoughtful compliance frameworks will successfully tackle the compliance complexities of 2025. They'll also position themselves as leaders in the IT channel for years to come.

The compliance crunch is here – and MSPs are perfectly placed to help solve it

MSPs must ensure their clients understand that the true value of CaaS lies not in offering a one-time fix, but in providing a sound framework from which ongoing compliance can be achieved more easily and effectively in a constantly shifting legislative environment.

BY ROSS DOWN, CHIEF REVENUE OFFICER, ISMS.ONLINE

ACROSS THE UK, organisations are facing an ever-heavier regulatory burden. Recently, the UK government outlined the scope of the new Cyber Security and Resilience Bill, which is set to come into effect later this year.

Specifically, the new Bill aims to strengthen the UK's cyber defences and better protect critical national infrastructure from digital threats.

However, achieving this will require more organisations to adhere to more stringent requirements.

It's the latest in a long line of expanding and evolving compliance obligations for UK organisations. Interestingly, tackling and reducing the legislative load has been on the government's agenda for a decade. The Business Impact Target (BIT) was introduced back in 2015 with the aim of reducing the cumulative costs of regulation on business. However, figures from the UK Regulatory Policy Committee show that steps have consistently been taken in the wrong direction, year after year. Rather than falling, regulatory costs rose by £7.8 billion during the 2017-2019 parliament, and a further £14.3 billion in the first three years of the 2019-2024 parliament. As a result, most companies are currently feeling the strain.

According to PwC's Global Compliance Survey 2025, 85% of firms feel compliance requirements have become more complex in the last three years. 82% said that this rising complexity has negatively affected senior leadership focus, while 81% believe it has impacted their transformation and change activities.

A multi-billion dollar opportunity for MSPs

In the face of these challenges, many companies are naturally seeking support and solutions.
There is good reason why Gartner predicts that investments in governance, risk and compliance tools are expected to increase by 50% between 2023 and 2026. Businesses shouldering the weight of growing compliance demands are looking for ways to alleviate the burdens.

For Managed Service Providers (MSPs), this presents a major opportunity.
For many companies, external partners and experts will be the first port of call.
At the same time, PwC's survey shows that cybersecurity, data protection and privacy are among the leading priorities for companies when it comes to compliance – areas where MSPs

are particularly well-positioned, thanks to their deep expertise and technical capabilities.

This presents a clear path for new revenue opportunities and service diversification. By adapting effectively and meeting the compliance needs of both new and existing customers as they evolve, MSPs will be able to grab a substantial piece of what is set to become a highly lucrative pie.

According to one estimate, the global Compliance-as-a-service (CaaS) market is set to be valued at $19.51 billion in 2030, up from $5.51 billion in 2022.
Developing a relevant CaaS offering
Of course, this isn't something that can be achieved overnight.

To capitalise on the opportunities effectively, MSPs will need to build a relevant offering with careful consideration, potentially making significant operational and cultural changes in the process.

At present, many MSPs provide technologies and digital solutions – an approach that will only work in part when it comes to CaaS. Where compliance is concerned, organisations can't simply overlay technologies within their existing operations. They also need to make operational changes that can have implications for people and processes.

MSPs will therefore need to ensure that their offerings account for this, providing the right combination of specialist support in addition to technologies to deliver the necessary results for clients.

Regarding the technology platforms themselves, MSPs must also consider several factors. Critically, it is important that any CaaS platform can integrate seamlessly with customers' existing technologies and systems.

If implementing a CaaS solution demands major infrastructure or operational overhauls, MSPs risk replacing one problem with another rather than truly solving their clients' challenges.

Then there is the question of transparency. Clients will want visibility over their compliance status, with the ability to monitor and assess changes and progress. Therefore, any CaaS platform must incorporate key user experience-centric features such as dashboards and reports that make it easy for clients to ascertain need-to-know information.

Highlight non-compliance risks vs compliance rewards

Once an offering is in place – supported by the right methodologies and technologies—MSPs can begin taking their CaaS solutions to market. To market any solution effectively, it's essential to clearly demonstrate its value.

In the case of CaaS, the most impactful approach is to highlight the contrast between the risks of non-compliance and the tangible benefits of achieving compliance.

Let's paint this picture.

For companies, non-compliance can lead to a variety of issues spanning everything from business disruption to productivity declines as well as fees and penalties. Further, the frequency of these impacts is increasing.
According to ISMS.online research, more UK companies are now being fined between £250,000 and £500,000 (26% today versus 21% in 2023), while many more are being fined between £100,000 and £250,000 (35% versus 18%).

On the flip side, compliance can do much more than help companies avoid penalties. In fact, the same ISMS.online research shows that this is the primary motivation for less than one in five companies. Far more talk about the role that compliance plays in helping them to remain competitive (34%), increase customer demand (34%), protect business (30%) and customer (29%) information and enter new markets and supply chains (27%).

This multitude of benefits is also reflected by the value that companies feel compliance offers.

Some of the most significant returns from investing in compliance include an enhanced business reputation (34%), direct cost savings from a reduced number of cybersecurity incidents (30%), time savings from more efficient security processes (29%) and greater appeal to investors looking for low-risk companies (28%).

Several other respondents also highlighted that compliance investments have enabled them to streamline their security infrastructure, making it easier and less costly to manage, while others said they've improved the quality of their business decisions.

Position CaaS as a long-term compliance strategy, not a quick fix
It's important, however, not to oversell CaaS as a 'set and forget' miracle solution.

MSPs must make it clear that while CaaS can help to reduce the burdens on companies in navigating various moving pieces of the legislative puzzle, compliance will still require ongoing and continuous management from the outset.

The total cost of compliance for UK companies has been growing consistently, and that's not expected to change anytime soon. Regulations both new and old will continue to emerge, evolve and change over time as new threats, challenges and opportunities arise.

Businesses, therefore, need to keep a pulse on the regulatory landscape, one way or another, adapting their compliance strategies as necessary.

For MSPs, it is important to ensure clients are aware of this, as well as the need to maintain proper audit trails, which can showcase their effective compliance efforts should regulators come knocking. Not only will documenting key processes show that compliance is being achieved. Equally, it will also help in managing legal disputes.

MSPs must ensure their clients understand that the true value of CaaS lies not in offering a one-time fix, but in providing a sound framework from which ongoing compliance can be achieved more easily and effectively in a constantly shifting legislative environment.

Those that position their services transparently, emphasising the benefits and best practices, will be better placed to build trust, deliver maximum value and grow alongside clients as the regulatory landscape evolves.

Turning compliance chaos into opportunity

How the channel can help businesses tackle cyber risk exposure under NIS2 and DORA.

BY CHRISTINA DECKER, DIRECTOR OF STRATEGIC CHANNELS EUROPE AT TREND MICRO

TWO MAJOR regulations have reshaped Europe's cybersecurity landscape in quick succession: the Network and Information Security Directive 2 (NIS2) and the Digital Operational Resilience Act (DORA).

Together, they are a a step-change in how governments expect organisations to manage cyber risk. The shift is especially significant for sectors dependent on digital infrastructure, where the stakes are high and the pressure is building. For many businesses – especially SMEs— these new rules present a number of challenges. However for the technology channel, they also represent a timely opportunity: to move from supplier to strategic advisor, helping clients navigate a more complex threat environment and build resilience into their operations.

Why the compliance stakes are rising

NIS2, which applies to a wide range of essential and important sectors, requires enhanced cyber hygiene, improved incident reporting, and a deeper focus on third-party risk. DORA, meanwhile, targets financial services and their ICT providers with even more specific obligations around operational resilience and business continuity.

Both regulations are a response to an increasingly sophisticated threat landscape. Cybercriminals have grown more organised and specialised, using automation, AI, and service-based models to scale their operations.

At the same time, organisations are more digitally interconnected than ever,

increasing their exposure to potential attacks.

This growing cyber risk exposure, the sum of digital assets, systems, suppliers, and users that could be exploited, is exactly what NIS2 and DORA aim to reduce. But our experience shows that many companies are falling short. Only some organisations are fully compliant with NIS2, and many that are claiming to be DORA-ready aren't even monitoring third-party suppliers, despite this being a core requirement. That leaves significant gaps – and major risks.

The role of cyber risk exposure

To meet the requirements of these regulations, organisations need to get serious about understanding their full cyber risk exposure. This isn't just about their internal IT environment – it includes cloud services, remote endpoints, contractors, and especially third-party vendors. Every external connection can become a potential entry point for an attacker.

Without full visibility across this ecosystem, it's difficult – if not impossible – to assess risk accurately, respond quickly to threats, or report incidents within the strict timelines that NIS2 and DORA demand. This is where many businesses are currently stuck. This is the moment for the channel to step up. Partners already know their customers' infrastructure, workflows, and weak points. That inside knowledge, combined with regulatory awareness, puts them in a strong position to advise clients on practical steps to reduce risk exposure and improve compliance posture.

That might mean helping map the digital supply chain, run regular risk assessments, identify overlooked assets, or implement clearer incident response plans. In many cases, it's not about selling new tools – it's about helping businesses use what they already have more effectively, while aligning it with regulatory expectations. For SMEs in particular, which may lack in-house security teams or the capacity to stay ahead of shifting compliance rules, this kind of advisory support is invaluable. It offers them not only guidance but peace of mind.

Continuous risk management, not one-off exercises

What NIS2 and DORA both make clear is that compliance isn't a project – it's a process. Cyber risk exposure must be monitored and managed continuously. Threats evolve, systems change, and suppliers come and go. Static security policies are no longer enough.

Channel partners can play a central role in establishing ongoing practices that address this dynamic risk. That might include:

- Regular reviews of third-party risk
- Asset discovery and inventory checks
- Incident response exercises and tabletop scenarios
- Governance reporting that maps risk to compliance
- Policy reviews and updates as regulations evolve

For partners who want to go further, offering these services on a recurring basis – whether through advisory retainers or managed offerings – can build stronger, more durable customer relationships.

From compliance burden to strategic opportunity

There's no question that the compliance burden is increasing. But so too is the opportunity for the channel to redefine its role. Rather than being just another vendor, partners can position themselves as protectors of business continuity and resilience.

By helping clients get a handle on their cyber risk exposure, channel partners not only assist in avoiding penalties or breaches – they empower businesses to operate with greater confidence and agility in a volatile environment.

NIS2 and DORA are not the final word on cybersecurity regulation. More rules are coming, and enforcement is only going to get tougher. Businesses that treat compliance as a tick-box exercise will continue to fall behind. But those that understand their risk exposure – and take proactive steps to manage it – will be in a far stronger position.

For the channel, this is a chance to lean in. Not with products, but with perspective. Not with tools, but with trusted guidance. The businesses that succeed in this new era of regulation will be the ones that understand the value of partnership – and the channel is perfectly placed to deliver it.

MSP Pulse-Check: has MSP 3.0 arrived?

At the start of the year, research firm Canalys set the tone with some bold predictions: the rise of MSP 3.0, which would include an AI-augmented channel, shifting customer behaviours, and a booming cybersecurity market. Now, with 2025 in full swing, it's fair to ask: how much of that forecast is fact, and how much is still fantasy?

BY STEVE PRESCOTT-JONES, DIRECTOR OF MANAGED SERVICES AT UBDS DIGITAL

SPOILER ALERT: MSP 3.0 is no longer just a talking point, it's happening. Significant change is occurring across the MSP sector, and many of the report's themes are playing out. But progress is far from consistent – or painless.

MSP 3.0 signals a shift beyond technical delivery to strategic enablement. While most MSPs still offer traditional services like first-line support, monitoring, and maintenance, there is a convergence between professional services and managed services. This is giving rise to a whole new raft of solutions, delivery models, and expectations, at a pace not seen before.

Buyers are changing - Fast. MSPs need to catch up

Today's buyers are increasingly digital natives: younger, more tech-savvy, and more confident in their understanding of IT. And while the report is right - this shift is having a big impact on the MSP sector - it's not necessarily in the way Canalys predicted.

Buyers now expect MSPs to operate differently. They want partners who behave more like DevOps teams, with daily stand-ups, agile delivery, and continuous iteration.

Customers don't want to spend days, weeks, or even months on impact assessments, quotes, and lengthy delivery cycles in the traditional MSP model. They expect time-to-value in days, sometimes even hours. MSPs are already adapting, driven by automation and AI. But the knock-on effect of this is that customers are demanding a leaner cost base and faster outcomes because they know AI is now built into many platforms. They don't want to pay a premium for business analysts or technical engineers to do what AI can increasingly handle.

AI is here – but only at the experimental phase

The AI hype is real. But as the report notes, so are the roadblocks. Real Agentic AI - where systems act autonomously on behalf of users - is not yet widespread, and it will take longer than just 2025 to reach maturity.

2024 was dubbed by many market watchers as 'the year of AI,' then quickly changed to 'the year of experimentation'. The hope was that 2025 would be when AI got real. So far, that hasn't fully materialised.

Despite the vendor noise and growing customer interest, few live implementations are in place. Canalys' figure that over 60% of partners still struggle to move AI projects beyond proof-of-concept feels accurate.

However, there's growing interest in Agentic AI. Self-healing servers and networks are already well-established and customers are now exploring concepts like service as software, where multiple AI agents chain together to perform tasks that, just 18 months ago, were too complex for automation.

However, costs remain high, and implementation is risky. With no clear market leader, customers are hesitant to invest, fearing vendor shifts or backing

MANAGED SERVICES SUMMIT LONDON

10.09.2025

CONVENE
155 BISHOPSGATE LONDON

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

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

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

INDUSTRY INSIGHTS

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

BREAKOUT SESSIONS

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

NETWORKING OPPORTUNITIES

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

INTERACTIVE EXPERIENCES

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Angel BUSINESS COMMUNICATIONS

Sukhi Bhadal	sukhi.bhadal@angelbc.com	+44 (0)2476 718970
Peter Davies	peter.davies@angelbc.com	+44 (0)1923 690211
Mark Hinds	mark.hinds@angelbc.com	+44 (0)2476 718971

IT EUROPA

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

https://london.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS IT EUROPA ANGEL EVENTS

the wrong horse. Still, the promise of Agentic AI is compelling and there will no doubt be a wave of real-world adoption and deal activity towards the end of the year.

Security is booming

Tech-savvy buyers are also far more focused on security, and that's been evident for several years. As the Canalys report highlights, customers don't want security as an add-on — they expect it built into every service. The forecasted 15% growth in managed security services is real — and a huge opportunity.

But in the era of MSP 3.0, the nature of security has changed. It's It's evolved from boundary protection of offices and data centres to enabling a secure but consistent frictionless experience from any device in any location to SaaS services via multiple layers of protection.

Today's security means pulling together multiple technologies to deliver integrated protection.

Security is now a board-level issue, driven by regulation and compliance, areas where customers expect MSPs to be fluent.

More than just an MSP

But customers want more than just integrated security. They expect knowledge of compliance, regulation, and vertical-specific risks. That's not just due to demographic shifts, but because the lines between IT, compliance, and cybersecurity are increasingly blurred — and that's reshaping the MSP value proposition.

Regulatory frameworks like DORA are game changers, especially in the finance sector. The implications of non-compliance are significant, and more customers are placing it at the top of their agenda. Insurance and legal risks are also growing, and customers are now expecting MSPs to understand and address those angles too.

While only a few MSPs are partnering with legal or insurance firms today, this broader expectation from customers is pushing the industry toward a more ecosystem-led approach.

What's next?

Although we are only part way through 2025, many of Canalys' predictions are already happening, albeit not necessarily quite as quickly or in quite the same way as the research firm has stated.

The evolution to MSP 3.0 is real. With the global managed services market set to grow 13% this year and hit $595bn, it's safe to say that this kind of scale doesn't come from sticking to the old playbook.

For MSPs, it's a time of transformation. But if there is one thing MSPs are experts in it's adapting to change. The winners will be those who embrace agility, align with emerging customer needs, and deliver outcomes that go beyond technology.

The smart MSPs aren't just waiting for MSP 4.0 - they're actively building it.

MANAGED SERVICES SUMMIT NORDICS

21.10.2025

STOCKHOLM WATERFRONT CONGRESS CENTER

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

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

INDUSTRY INSIGHTS

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

NETWORKING OPPORTUNITIES

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

INTERACTIVE EXPERIENCES

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Angel BUSINESS COMMUNICATIONS

Sukhi Bhadal sukhi.bhadal@angelbc.com +44 (0)2476 718970
Peter Davies peter.davies@angelbc.com +44 (0)1923 690211
Mark Hinds mark.hinds@angelbc.com +44 (0)2476 718971

IT EUROPA

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

https://nordics.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS IT EUROPA ANGEL EVENTS

Multi-tenancy: a global necessity for the modern MSP

In a digital world that demands more from technology partners every day, multi-tenancy is not just a smart choice. It is the foundation of the modern MSP business model worldwide, and especially in the US, where innovation, compliance, and scalability must go hand in hand.

BY YORAM NOVICK, CEO, ZADARA

THE PACE of technological change is redefining how businesses operate, compete, and serve their customers. For Managed Service Providers (MSPs), this means navigating a landscape shaped by rising client expectations, tightening regulations, and an urgent push for both efficiency and sustainability. To stay ahead, MSPs must adopt strategies that enable scale without compromise – and one of the most impactful among them is multi-tenancy.

What began as an architectural approach favored by hyperscale providers has now become a cornerstone of modern IT delivery. Multi-tenancy enables service providers to host multiple customers on a shared infrastructure while ensuring strict separation of data and operations, and upholding individual Service Level Agreements (SLAs) for each customer. For MSPs focused on growth, resilience, and customer satisfaction, this model is proving essential.

Global momentum and regional drivers

The demand for multi-tenant environments is accelerating around the world, driven by a range of regional priorities. In Europe, compliance, data privacy, and digital sovereignty are at the forefront. In the United States, enterprises are rapidly expanding digital operations and seeking cloud-native solutions that balance performance, compliance, and cost-efficiency. Growing concerns around cybersecurity, federal and state-level data regulations like CCPA and HIPAA, and increasing cloud adoption are all influencing infrastructure decisions. Meanwhile, in the Asia-Pacific region, fast-paced digitalization and smart city initiatives are fueling investments in agile infrastructure.

According to industry forecasts, the global multi-tenant data center market is on track to reach over USD 50 billion by the end of the decade. In North America alone, multi-tenant colocation and cloud infrastructure demand is rising sharply as enterprises seek to future-proof operations and reduce IT complexity. This global momentum signals not just a shift in infrastructure preferences, but a fundamental change in how IT services are consumed and delivered across continents.

Cost efficiency for providers and customers

One of the most immediate advantages of multi-tenancy is cost efficiency. Traditional single-tenant models require a dedicated set of resources for each customer. That means more hardware, more software licenses, more maintenance, and more energy usage – all of which drive up costs.

Multi-tenancy improves utilization by enabling providers to share infrastructure across customers without sacrificing performance or security thereby reducing capital and operational expenses. MSPs benefit from better margins, while customers gain access to enterprise-grade services at a fraction of the typical cost.

Scalability without complexity

Today's businesses are fluid. Whether scaling for growth, launching new services, or adjusting to seasonal demand, clients expect their IT infrastructure to adapt quickly. MSPs must be able to deliver flexible capacity without introducing operational complexity.

Multi-tenant platforms allow for rapid provisioning, dynamic resource allocation, and seamless updates. New customers can be onboarded quickly, and existing ones can scale their services up or down in real time. This elasticity is particularly valuable in industries experiencing fast-paced digital transformation, including finance, healthcare, manufacturing, and retail.

Security and compliance in a shared model

Security remains a top concern for MSPs and their clients, whether they're operating in the U.S. under HIPAA or CCPA, in the EU under GDPR, or in APAC regions with growing data localization requirements. Fortunately, modern multi-tenant environments are built with security at their core.

Each customer's data is kept separate and encrypted, often using customer-controlled keys. Access controls are precisely managed, and systems are continuously monitored for vulnerabilities or anomalies.

This level of protection supports compliance with a wide array of global data protection laws, offering clients the confidence they need to trust shared environments. In the U.S., where security concerns are intensifying amid rising ransomware and supply chain attacks, robust multi-tenant security architectures are becoming a competitive differentiator.

Operational simplicity and centralized control

Maintaining isolated environments for each customer may offer clarity, but it also introduces significant operational overhead. Routine tasks like patching, monitoring, and reporting can become repetitive and inefficient across a large customer base.

Multi-tenancy simplifies these processes through centralized management. With a single dashboard, MSPs can oversee all clients, apply updates at scale, automate workflows, and gain insights into system performance. This centralized control improves efficiency for the provider and enhances the overall experience for the customer.

Sustainability through smarter infrastructure

Sustainability is now a global business imperative. Governments and enterprises worldwide are under pressure to meet environmental standards, reduce carbon footprints, and improve ESG performance.

In the U.S., rising energy costs and SEC-proposed climate disclosure rules are pushing companies to embrace greener infrastructure. Multi-tenancy directly supports these goals.

By consolidating services on shared infrastructure, MSPs reduce energy consumption and limit the environmental impact of underutilized systems. Fewer physical servers mean less power, less cooling, and fewer resources wasted. It also enables smarter lifecycle management of hardware, contributing to more responsible and sustainable operations.

Delivering a cloud-native experience

Today's customers want more than just reliable service. They want a user experience that is fast, seamless, and intuitive – just like the cloud platforms they already use.

Multi-tenancy makes it easier for MSPs to meet these expectations while retaining control over data location, security policies, and regulatory compliance. The model supports rapid iteration, standardized service tiers, and customization when needed. Clients get the performance and agility of cloud services without vendor lock-in, while providers maintain the flexibility to evolve alongside customer needs.

Preparing for the future of managed services

The MSP role is evolving from backend support to strategic partner. Clients increasingly rely on providers not just to maintain systems, but to drive innovation, improve efficiency, and guide transformation. To succeed in this new era, MSPs need infrastructure models that support scale, simplicity, and security.

Multi-tenancy offers exactly that. It creates a foundation that is efficient to operate, straightforward to manage, and flexible enough to serve clients of all sizes, regardless of location or industry. For providers aiming to grow, compete, and lead, it represents a critical capability that enables long-term success.

In a digital world that demands more from technology partners every day, multi-tenancy is not just a smart choice. It is the foundation of the modern MSP business model worldwide, and especially in the US, where innovation, compliance, and scalability must go hand in hand.

Unifying automated security to overcome IT middle management challenges

MXDR helps tip the balance of power away from threat actors and in your favour. Working with a digital managed service provider gives you the guidance and support to take the right steps and strengthen your security posture.

BY MIKE FRY, INFRASTRUCTURE DATA & SECURITY SOLUTIONS DIRECTOR AT LOGICALIS UK&I

TODAY'S cyber threats are faster, smarter, and harder to detect. This means IT security teams must have visibility across all corners of the IT estate from staff devices, external locations containing company data, communication apps and the network foundation of a business.

The digital-first world we operate in today puts relentless pressure on IT security managers like you! You're expected to keep your team's skills sharp, plug any knowledge gaps, and still protect the business from ever-evolving threats.

Insufficient security resources remain a major challenge. While you may have tools for certain areas, such as endpoint protection, you might still have blindspots to unknown security flaws elsewhere.

Even when running multiple tools at once, limited integration and visibility of each other can cause alert overload and create critical gaps in protection.

When those tools flood you with

information and notifications, it can be overwhelming and lead to fatigue or missed alerts of major threats to the network.

This is where managed extended detection and response (MXDR) comes into play. A unified approach to automated security, deployed across your entire IT estate, is the key to complete protection and peace of mind.

The benefits of XDR and why they matter

To begin with, before we consider MXDR, let's clearly define what extended detection and response (XDR) entails and how it can support you in overseeing security protocols.

At its core, XDR is a holistically unified technology that provides real-time threat detection and response across communication, endpoints, networks, and the cloud. It helps identify and mitigate threats before they cause significant damage.

As a result, XDR protects against emerging threats and helps stay one step ahead of threat actors, eliminating blind spots that would otherwise go unnoticed.

Here's what you can expect:

- Faster threat detection results from a greater understanding of particular vulnerabilities and risk areas.
- Prioritised threats by impact, allowing for greater focus on the most pressing dangers to the business, and lowered strain in the process.
- Accelerated investigations through awareness of the full scope and entry vectors of attacks.
- Accelerated response, aided by AI and machine learning, along with remediation recommendations.

To complicate matters further, the constant evolution of cyber-attacks means that security teams need to also constantly evolve and sharpen up their defence capabilities - this means your staff could be constantly playing catch-up.

As an IT security manager juggling the daily responsibilities up and down the chain of command, XDR helps minimise this juggling act.

Overcoming skills gaps with MXDR

XDR alone is powerful. But when it's managed by a trusted partner, it becomes a game-changer.

To complicate matters further, the constant evolution of cyber-attacks means that security teams need to also constantly evolve and sharpen up their defence capabilities - this means your staff could be constantly playing catch-up. Using AI and machine learning tools working in tandem can help close skills gaps and keep evolving threats at bay.

The 'managed' aspect of MXDR refers to an extended detection and response team brought in as a service. MXDR adds a 24/7 Security Operations Centre (SOC) to the mix – giving you access to experienced analysts, real-time monitoring, and rapid incident response, without the need to build or manage it all in-house.

Crucially, this eases the strain on your internal team, helps address skills shortages and allows you to focus on strategic priorities such as improving access controls, reviewing policies, or enabling training, without living in fear that something's being missed.

Having these new data capabilities is also likely to boost buy-in from the C-suite, especially those who may be hesitant about investing in new security tools, but are aware of the risk to the firm's reputation.

The Logical step forward

Partnering with a managed security provider takes the burden off you and your IT security team. It gives you clear visibility, faster resolution and fewer sleepless nights. No more juggling tools. No more missed alerts.

You no longer need to be pulled away from your regular responsibilities to play the role of full-time security analyst - a role you likely didn't sign up for.

MXDR helps tip the balance of power away from threat actors and in your favour. Working with a digital managed service provider gives you the guidance and support to take the right steps and strengthen your security posture. That means no more blind spots and no more playing catch-up.

Strategies for managing context switching and increasing productivity

A common difference between CISOs and vCISOs is vCISOs' need to context switch. Part of the job requires the ability to juggle multiple clients, their tasks and security roadmaps. This constant juggling, which is also known as "context switching" is a silent productivity killer. It can even cost a provider business sustainability and stunt future growth.

BY DROR HEVLIN, CHIEF INFORMATION SECURITY OFFICER, CYNOMI

THERE ARE tools and technologies that can be used to provide vCISOs the solutions they need in order to avoid context switching and mitigate the challenges involved with managing multiple clients' security. These tools can drive efficiency, help provide better security and compliance services and even create opportunities for scaling.

A context switch is when a computer's operating system changes from executing one task to another. In order to accomplish this, the computer saves the state of the current task and loads the new one, so that the CPU can execute it. While this is a key feature of modern operating systems, it also has a negative impact on system performance.

Similarly, when humans go through the mental process of shifting focus from one task, topic, or activity to another quickly, it also negatively affects performance. We have to reorient our attention, recall details about the new task and re-engage with it. This could result in reduced productivity, increased errors, as well as stress and fatigue. This whole process is draining because our brains must drop the current task and pick up where we left off on the new one, creating a cognitive load. Some of our focus may remain tied to the previous task, slowing down performance on the new one, not to mention that it takes time to re-familiarize ourselves with the new task or context.

According to Gloria Mark, Professor in the Department of Informatics at the University of California, Irvine, it can take 23 minutes to refocus after a task switch. If you're juggling multiple priorities, this adds up, resulting in fewer deliverables within the same time frame.

The diverse, dynamic and technological nature of security and compliance responsibilities makes context switching particularly challenging for vCISOs. For each client, vCISOs have to deal with unique tech stacks and product roadmaps, security technologies, tools and frameworks, risk tolerances, security maturity levels, threats and vulnerabilities, compliance regulations (if you're working in different industries), security plans, stakeholders: IT, executives, auditors, strategic business priorities and culture.

Like any other external consultant, vCISOs work with multiple organizations, requiring the ability to hop between different clients, tasks and details.

This means that vCISOs need to be able to manage multiple concurrent security and compliance priorities. For example, incident response planning for one client, compliance reporting for another and strategic

discussions with C-level executives for a third. All while adapting them to each organization's risk appetite, business strategy, regulatory requirements, IT architecture and culture. They also need the ability to govern the use of multiple tools across different environments.

vCISOs need to uphold each client's security posture and planning. This includes knowing the details of existing gaps, creating and managing the plan to overcome them and overseeing the progress. Just as importantly, vCISOs need to be able to adapt their communication, tone and technical depth style for each stakeholder in each company. This might mean interacting with dozens of people in a professional context on a weekly basis.

The cybersecurity field is evolving quickly, with new threats and vulnerabilities emerging daily. vCISOs need to be able to translate the impact of these risks to each client's ecosystem, as well as the new tools and technologies evolving to address them. While these are all complexities in-house CISOs face as well, their focus is on one company.

This means one CEO, one risk assessment to address, one architecture, one business culture and one security posture to improve. They hold the complete company picture and are immersed in it. vCISOs, on the other hand, deal with multiple such perspectives, and sometimes only have a limited view into the inner workings of the company.

How context switching affects your business

Context switching is more than just an inconvenience. It carries significant impacts. First, there's the security impact. Frequent context switching increases the likelihood of inconsistencies and errors, such as applying incorrect policies or overlooking specific client requirements.

These can result in misconfigurations, not patching on time, leaving vulnerabilities and more. On a more strategic level, mental fatigue can reduce the ability to make the right security decisions that will bolster clients' security posture. Long term effects of content switching can also lead to burnout, diminished job satisfaction and lowered client outcomes.

The business impact of context switching also impedes your ability as a vCISO to maintain and grow your business. If clients perceive that your attention is divided and that communication is inconsistent, or they sense recurring errors, they may feel their security is not a priority. This can damage relationships and confidence in your ability to protect their organization. This could result in the loss of a client, as well as the potential referrals that client could bring by recommending you to others.

Reducing context switching is crucial if you want to maintain productivity, ensure strong security outcomes and grow your business. Here are some useful and impactful tips to follow:

Prioritize tasks based on risk and impact

Start with the tasks that bring the most value and impact. Evaluate tasks and incidents based on their security implications and urgency. You can also use a risk register to help prioritize them and support your decision-making. Address high-risk tasks and active threats before routine activities. Answer C-level queries before tactical questions. Create reports to show posture and ongoing progress before moving on to the next security pillar unless it's an active threat.

Put Similar Activities Together

One of the biggest challenges of mental shifting is refocusing on different types of tasks. Deep work like learning about a new compliance framework requires different cognitive skills than answering emails. Perform similar tasks in dedicated blocks of time to reduce mental shifts. For example, review all client security dashboards during a morning session, then focus on client communications in the afternoon. This will have a noticeable impact on productivity.

Choose effective communication practices

When you are in the zone of crafting a new client strategy and are interrupted by an alert for a client meeting right in the middle of your work can actually kill the whole creative process. Encourage clients to provide updates or requests in writing, allowing you to respond during planned intervals. Meetings are still important, so schedule regular check-ins either weekly or bi-weekly, to check in and address their needs, while reducing ad hoc meetings and interruptions.

Put it all in writing

Replicability and standardization in your everyday work can reduce friction. Keep detailed playbooks and set processes for common scenarios like incident response, compliance audits, or vendor assessments, as well as detailed notes for each client. These can help streamline processes while also enabling you to share them with other team members, so they can perform them instead of you, which will then reduce your cognitive load.

Build effective teams and delegate

You can accomplish this by building small, specialized teams for each client and assign the team members routine security tasks. By delegating operational tasks such as scheduling or documentation to team members or external vendors, you can then focus on more strategic priorities. Utilize automation tools for routine reporting or vulnerability monitoring.

Use a vCISOplatform

A vCISO platform is an automated platform that provides and generates everything required to provide vCISO services at scale. This includes risk and compliance assessments, security gap analysis, tailored policies, strategic remediation plans with prioritized tasks, tools for ongoing task management and risk management, security progress tracking and customer-facing reports.

A vCISO platform acts as the central cybersecurity and compliance management hub and is the one source of truth for the vCISO, for each client individually and for all clients together.

A vCISO platform allows vCISOs to easily create and manage multiple clients. They can track security and risk postures, monitor compliance and security framework complacency, prioritize and manage tasks, allocate resources and generate reports that quickly show the value of their vCISO services. All of these things can be done from a single dashboard for all clients.

These capabilities take away most of the challenges of vCISO context switching:

- Priorities and current security and compliance statuses for each client are clearly presented and managed. vCISOs are always updated on the latest mapping, gap, task status or progress, without the delay that accompanies retrieving the information.
- This also makes it easy for vCISOs and teams to understand what to work on next. Rather than having to remind yourself about important gaps to address or what was the next task discussed with the client, the information is readily available.
- Switching between clients also becomes easier. Comprehensive visibility into all clients from a single dashboard eliminates the need to switch between tools used to manage each client separately.
- A single dashboard of all clients and their current gaps and task management status makes it easy to prioritize clients and see which one to address next.
- Communication with stakeholders is also simple and streamlined, since reports are easily generated and any question can be answered in just a few clicks.
- Unlike a spreadsheet or emails, automations and standardizations eliminate the need to manually update client accounts or employees, alleviating one more task to (context) switch to.
- Finally, a high quality of work is ensured through the security and compliance tasks the platform takes care of, like generating policies.

Anyone on the team can quickly use the platform, enabling easy delegation of tasks and the workload. Productivity will increase due to automations and standardizations when performing security and compliance tasks increases productivity and grows revenue.

And the bonus? Seeing the full picture of clients' security gaps helps vCISOs upsell their services that can address those gaps, which will help to grow the business and increase revenue.

Context switching drains productivity and focus, especially for vCISOs juggling multiple clients, frameworks and stakeholders. It is possible to permanently put an end to context switching and increase focus on what is important and will have the most impact.

When you do this, you will see a dramatic increase in performance and skyrocketing business growth. Emerging tools built for vCISOs can automate status updates, map controls to frameworks, and track tasks across clients. AI-powered assistants can also help summarize alerts, extract insights, and prioritize based on severity.

To be truly effective, a vCISO needs to go beyond putting out fires. Minimizing context switching is critical for strategic thinking, maintaining security quality across clients, and staying mentally sharp. By adopting smarter workflows and leveraging the right tools, vCISOs can reclaim their focus, and deliver even more value.

MANAGED SERVICES SUMMIT MANCHESTER

18.11.2025

MANCHESTER CENTRAL
MANCHESTER UK

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

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

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

INDUSTRY INSIGHTS

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

NETWORKING OPPORTUNITIES

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

INTERACTIVE EXPERIENCES

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Angel BUSINESS COMMUNICATIONS

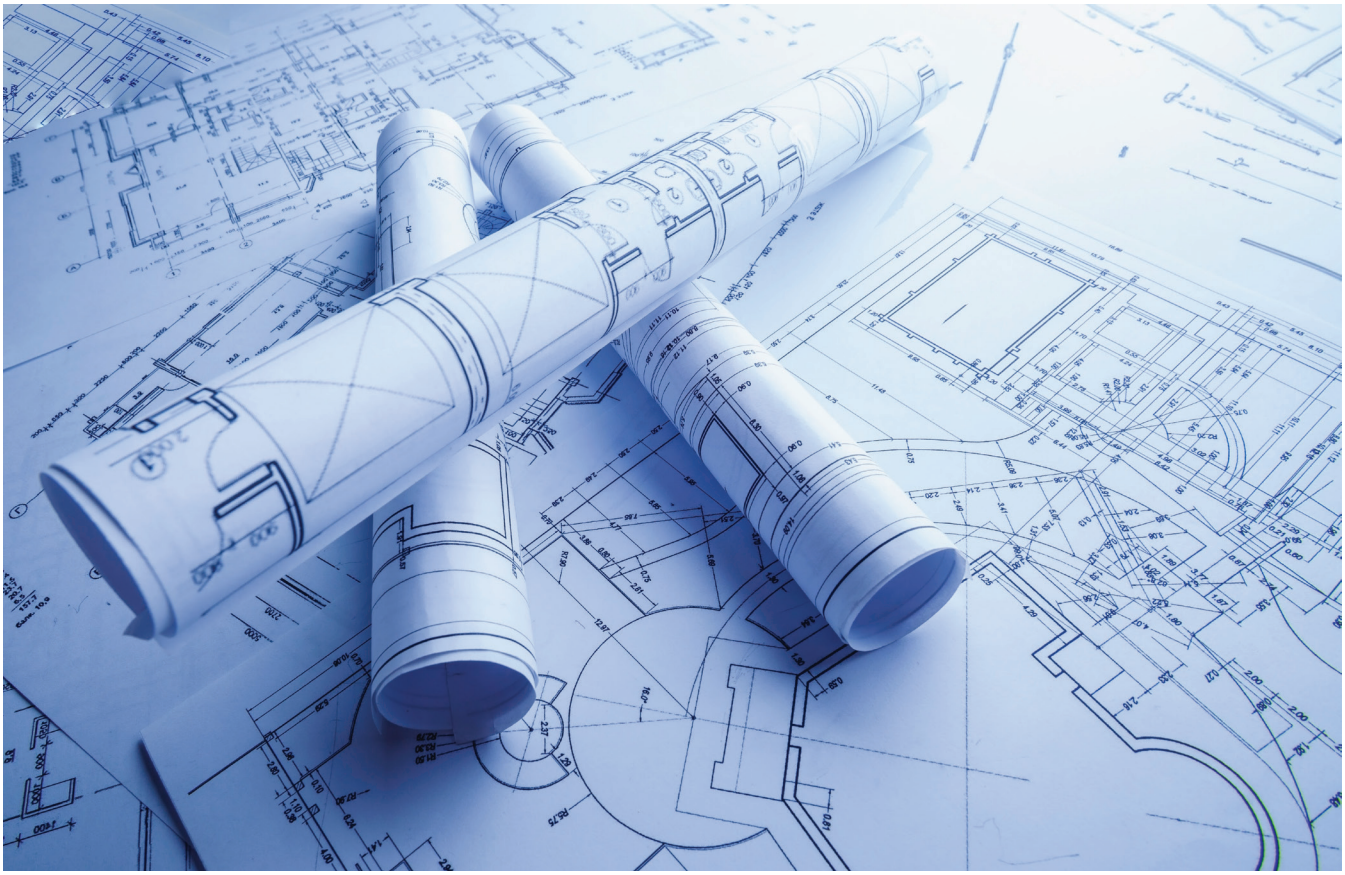
Sukhi Bhadal sukhi.bhadal@angelbc.com +44 (0)2476 718970
Peter Davies peter.davies@angelbc.com +44 (0)1923 690211
Mark Hinds mark.hinds@angelbc.com +44 (0)2476 718971

ITEUROPA

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

https://manchester.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS ITEUROPA ANGEL EVENTS



Securing MSPs: the blueprint for cyber resilience

It often seems as though the advice on how to stay secure is obvious but it's amazing how many organisations and individuals don't do the basics. Sometimes the most obvious steps are the most effective in keeping organisations secure. You don't have to be the most cyber-secure MSP but definitely don't be the least.

BY ADAM PILTON, SENIOR CYBERSECURITY CONSULTANT AT CYBERSMART

MANAGED SERVICE PROVIDERS (MSPs) play a vital role in modern business operations, allowing organisations to outsource services like cybersecurity and IT. This gives organisations, especially small and medium-sized enterprises (SMEs), an easy way to remain cyber secure without needing a full-scale in-house team.

However, their position as a gatekeeper to several client systems has made them a prime target for cybercriminals, as shown in a recent survey revealing that 76% of MSPs spotted a cyberattack on their infrastructure within the last 12 months. Recent attacks on MSPs have highlighted the detrimental effect cyberattacks can have on several organisations in a short period and, given the increasing reliance on MSPs, emphasises the need for robust cybersecurity practices to be adopted.

Why do cybercriminals target MSPs?

On the surface, an MSP might seem an odd target for cybercriminals as they've often implemented the most secure cybersecurity tools, processes and policies. Yet, cybercriminals continue to attack them. Why?

It's down to the potential reward of gaining access to the systems and networks under an MSP's control. Not only this, but if a hacker can breach an MSP, they'll have access to data including everything from employee login details to financial records.

Ultimately, attackers target MSPs for the same reason they target supply chains. If you can successfully breach their defences, you'll gain access to reams of sensitive data. And, the more data they

have, the more money there is to be made from ransomware.

Consequences of a successful attack on MSPs

For MSPs, the consequences of cyberattacks can be divided into direct and indirect.

- **Direct Consequences**
  There are several direct consequences of an attack including serious disruption to systems. Unless an attack is caught and dealt with early, an attack can inject malware and bring down an MSP's systems. This often results in a long process to fix and restore the affected systems before going back online. This not only impacts productivity but also can dent employee morale.

  A successful ransomware attack can also result in locked systems and/or stolen data. This leaves SMEs with little choice other than to pay the ransom or risk allowing private customer details to be shared online. This would most likely lead to a reputational hit, making it harder to retain and win clients.
- **Indirect Consequences**
  There are also the damaging effects of indirect consequences which often see an MSP's clients suffer more than the MSPs themselves, especially SMEs. A recent government survey found that only 33% of SMEs use threat monitoring tools and even fewer (31%) conducted a cybersecurity risk assessment in 2024. This leaves SMEs much more susceptible to threats than large organisations and shows how reliant they are on MSPs to keep their organisation secure. There are several examples of successful cyberattacks such as the Kaseya ransomware attack which spread to dozens of MSPs and over 1,500 of their customers in a matter of hours highlighting why the risk for attackers is worth it for the extensive rewards.

How to protect against MSP cybersecurity threats

There are several measures an MSP should adopt to protect themselves and their customers. The majority of these measures are relatively simple to implement and yet, so few organisations actually take action. The first step is to install software patches. All software, even the best-protected, can develop vulnerabilities over time which presents opportunities for attackers. Attackers work efficiently and will target the organisation with the weakest defences so don't let that be you.

Mult-factor authentication (MFA) is another simple way to improve security for your employees and ultimately reduce risk. Passwords alone are vulnerable, but MFA makes things much more difficult for an attacker to breach. Alongside usernames and passwords, adding security questions, PIN codes and biometrics such as thumbprints will massively reduce your organisation's chances of suffering a breach.

It is also vital to back up your data as a failsafe if you do suffer a breach. In some cases, it can even help to avoid paying ransom to retrieve your missing data. The easiest method is to install data backup software which will automatically create and store copies on an external source for safekeeping. A worrying 55% of data breaches are caused by human error so with this in mind, one of the most important strategies to counter cyber attackers is to train staff on the risks and how to stay secure. There are simple ways to train employees, or you could use a security awareness training provider to give your employees the best education in staying secure. Either way, it is vital that all members of staff are given as much support as possible to reduce risks.

Finally, it is important to create an incident response plan. Cyberattacks aren't inevitable, but they are statistically likely, so an actionable response plan is crucial. This will give employees a clear set of instructions to follow during and after a cyberattack which can help to minimise the damage to an organisation. It is also smart to encourage MSP clients to develop their own response plan as just 4% of MSPs say their clients have a plan in place. Following these steps does not guarantee total security from breaches, but they will help to reduce the chances significantly which will save an organisation time and money.

Stay on top of MSP cybersecurity

It often seems as though the advice on how to stay secure is obvious but it's amazing how many organisations and individuals don't do the basics. Sometimes the most obvious steps are the most effective in keeping organisations secure. You don't have to be the most cyber-secure MSP but definitely don't be the least.

The strategic role of channel partners in enterprise cyber resilient storage solutions

A significant transformation is underway in many manufacturing enterprises, triggered by greater interaction between Operational Technology (OT) and IT systems. Channel partners should be aware of how this trend has implications for cyber security and help their clients to mitigate the risks. Sharing insights like these creates an opportunity to add more strategic value during consultations and strengthen the trusted technology partner relationship. Here's why.

BY JAMES (JT) LEWIS, DIRECTOR OF CHANNEL OPERATIONS FOR EMEA AND APJ AT INFINIDAT

Traditionally, OT systems have focused on controlling physical processes and equipment. In contrast, IT systems handled data processing and business operations. These two systems have evolved in recent years and the traditional separation between the two is very rapidly disappearing, as manufacturers embrace digital transformation and Industry 4.0 to drive efficiencies. The result is an integrated approach that enables real-time monitoring and data analysis, improved efficiency and enhanced productivity across the entire manufacturing operation. It means communication between shop floor operations and enterprise-level systems is seamless, leading to better decision-making and better optimised production processes.

The Manufacturing Execution System (MES) lies at the heart of the integration between OS and IT. It supports the planning, monitoring, documentation and control of manufacturing processes in real-time. It also links higher-level ERP systems and industrial automation systems through process and machine control systems. Data flows seamlessly between production equipment and business systems, allowing for comprehensive visibility and optimisation of manufacturing processes. Enterprises can now make data-driven decisions based on real-time information, significantly enhancing their operational capabilities. This offers huge advantages to manufacturers, but integration also brings many risks and vulnerabilities - which channel partners, in their role as trusted technology

partners, should be communicating to clients.

One of the biggest risks is a potential data breach/cyber threats and new research from Deloitte conducted with the Manufacturing Leadership Council in 2024 quantifies this. The study reported that 48% of manufacturers experienced at least one data breach in the past 12 months, with an average cost of £2.1 million per breach. By helping manufacturers to understand these risks comprehensively, channel partners have a unique opportunity to position themselves as strategic advisors rather than just technology vendors, creating stronger, more successful long-term relationships.

Integration brings vulnerability

As OT and IT systems become interconnected, they also become more vulnerable to cyber threats that specifically target enterprise storage systems. According to a 2024 survey by industry research firm Omdia, 80% of manufacturing firms had experienced a significant increase in overall security incidents and breaches in 2024. The same study also found that less than 50% of manufacturing firms are prepared for the threat of these cyber security breaches, leading to significantly increased risk. This is critical because data is one of a manufacturing company's most valuable assets. With enterprises globally suffering an average of >1,650 cyberattacks per week, it is not a case of if you will suffer a cyberattack, but when, and how often.

Devastating impact of storage targeted attacks

A ransomware attack on enterprise storage systems can cripple a manufacturer, completely halting production processes as data and files become encrypted and inaccessible. Such an attack can also compromise the entire manufacturing operation, from design and engineering data to supply chain management information.

If key files are encrypted, the enterprise may not have access to product specifications, production schedules, and customer orders. Operations can be brought to a standstill and the implications are far reaching, potentially also damaging long-term projects, customer relationships and the business reputation.

The cyber security landscape has now evolved to a point whereby expecting to completely prevent a cyberattack is unrealistic. Cyber criminals are continuously refining their techniques, often applying social engineering and phishing campaigns that bypass traditional security measures. This means manufacturers need to shift the focus away from prevention alone to ensuring a rapid recovery when, and not if, a cyberattack occurs

Data published by the manufacturing industry body, Make UK, corroborates this. Its most recent report published in 2023 highlighted that during the previous year, nearly half of British manufacturers suffered cyberattacks. A quarter of affected companies reported losses ranging from £50,000 to £250,000, but the financial implications were just one aspect of the problems encountered - 65% also experienced production downtime and a further 43% faced reputational damage.

That's not all. Modern ransomware attacks have evolved beyond simple encryption to also include data exfiltration. Sensitive intellectual property and proprietary manufacturing processes can be stolen and sold on dark web marketplaces, causing long-term damage to an enterprise's competitive position. Furthermore, if personally identifiable information is compromised during these breaches, manufacturers may face significant regulatory penalties under frameworks like GDPR.

Switch from prevention to recovery

The cyber security landscape has now evolved to a point whereby expecting to completely prevent a cyberattack is unrealistic. Cyber criminals are continuously refining their techniques, often applying social engineering and phishing campaigns that bypass traditional security measures. This means manufacturers need to shift the focus away from prevention alone to ensuring a rapid recovery when, and not if, a cyberattack occurs.

This shift in perspective is particularly critical because cyber criminals typically don't discriminate between targets based on company size or industry prominence. Any enterprise is fair game. Small, regional manufacturers face the same sophisticated threats as multinational corporations, so ensuring cyber resilience across the entire manufacturing sector is essential.

Cyber resilience is also a regulatory requirement

Depending on the scope of an enterprise's business operations, cyber resilience may also be a legal requirement. In the EU, manufacturers must comply with the NIS2 directive (2024). The situation for UK manufacturers is more complicated because although NIS2 does not directly apply to all UK companies due to Brexit, it may apply if they have operations or customers based in the EU. This is equally true if a manufacturer has operations in the US or Japan – both of which have similar cyber regulations to the EU and the UK.

In addition, the UK continues to operate under its own NIS Regulations (introduced in 2018) and is updating its cyber security framework through the upcoming Cyber Security and Resilience Bill. This Bill is expected to be presented to Parliament later in 2025. Clearly, what all manufacturing enterprises need now more than anything is the strategic guidance to develop a cyber resilient storage infrastructure. Channel partners could be adding significant value here by sharing these foundations.

Five foundations for cyber resilient storage

A cyber resilient storage infrastructure to support manufacturing business continuity is built on five key principles:

- **Immutable snapshots**

Rather than creating simple backups, manufacturers need secure, unalterable

data copies taken at specific intervals. These immutable snapshots ensure that critical production and business data remains unchanged after creation, providing a reliable recovery source regardless of attack sophistication.

Logical and remote air-gapping
Effective cyber resilient storage requires logical isolation of immutable snapshots from network access. Air-gapping - implemented locally, remotely, or both - creates an additional protection layer that keeps recovery data segregated from potential infection vectors.

Automated detection and response
The speed of modern cyberattacks renders manual monitoring insufficient. Manufacturing companies need automated cyber security capabilities that integrate seamlessly with their existing security stack, including Security Operations Centres (SOC), Security Information and Event Management (SIEM), and Security Orchestration, Automation and Response (SOAR) platforms. These systems should automatically trigger immutable snapshots when security incidents are detected.

Fenced forensic environment
Recovery from cyberattacks requires a completely isolated network environment for forensic analysis. This "fenced" area allows for thorough data testing and integrity verification, ensuring that recovered data isn't compromised before reintroduction to production systems.

Near-instantaneous recovery
Critical for manufacturing operations is the ability to retrieve clean data copies within minutes, regardless of dataset size. Manufacturing processes are particularly time-sensitive, making rapid recovery capabilities essential for minimising production disruption and financial losses.

Storage decision making gets strategic

The basic principles of building a cyber resilient storage infrastructure may be well-understood, but a successful implementation is more challenging.

It calls for a strong strategic technology partnership between technology vendors, channel partners and the end user enterprise. When evaluating a storage vendor, manufacturing companies should look beyond the traditional criteria, like capacity, speed, price/performance-ratio, and the availability of a flexible consumption model. Channel partners can help customers perform this analysis and potentially also support the final implementation process.

Today's threat landscape demands a more strategic approach, with equal consideration to cyber resilience capabilities. And when supported by partners to implement a comprehensive cyber resilient storage infrastructure, manufacturers can protect their most valuable asset – data - while ensuring business continuity, even in the face of sophisticated cyberattacks.

AI-ready data: your best enterprise asset

Without structured, governed data, your AI will never deliver on its potential. But with it, your data will become the competitive edge that powers your future.

BY JESSE TODD, CEO OF ENCOMPAAS

TODAY'S enterprises are awash in data. Emails, documents, spreadsheets, chat logs, videos, images — these unstructured assets make up 70-90% of an organisation's data, according to Gartner. And while this content is often overlooked or siloed across repositories, it holds immense value – if only it could be unlocked.

Though such data may seem trivial, hidden in unstructured data are the insights that drive smarter decisions, operational efficiency, and innovation. An email exchange may reveal unmet customer needs. A forgotten file might contain critical compliance information. A misfiled document in a shared drive could expose sensitive employee or customer data. But without structure or governance, these assets remain chaotic and unusable — and that's a major problem for organisations investing in AI.

Because the truth is simple: AI fails when data is a mess.

Generative AI tools are only as good as the data that feeds them. If that data is scattered, unstructured, or riddled with risk, the results will be unreliable, inaccurate, and potentially harmful. Feeding raw, ungoverned data into AI is like asking a new hire to analyse customer satisfaction using a pile of disorganised customer contracts — without any context or clarity, the answers are bound to be wrong.

It's no surprise, then, that 60% of business leaders lack confidence in their data-AI readiness to realise business value from GenAI, despite 79% expecting it to deliver competitive advantage within the next 18 months.

That's why AI-ready data is rapidly becoming an enterprise's most valuable asset.

AI-ready data isn't just clean. It's contextualised, permissioned, labelled, and organised. It's governed in line with compliance requirements. It's discoverable and enriched. And when your data reaches this state, AI can finally do what it promises: deliver accurate, actionable insights that leaders can trust.

Embracing intelligent information management solutions, like those offered by EncompaaS, can solve this very challenge. By transforming chaotic, unstructured content into a structured, governed knowledge base, organisations can establish a foundation of high-quality, AI-ready data.

When information is discovered, enriched, and normalised across repositories, it becomes a trustworthy knowledge resource – enabling AI to deliver accurate, reliable and repeatable outcomes.

With AI-ready data in place, organisations can unlock previously untapped business intelligence, optimise operations, identify new revenue streams, and bring improved products and services to market faster. They gain the visibility to see trends and risks before competitors do — and the confidence to use AI in high-stakes decisions.

As data volumes explode and AI evolves at a rapid pace, ignoring unstructured data is no longer an option. Intelligent information management platforms help organisations take control of their data and prepare it for what's next.

Without structured, governed data, your AI will never deliver on its potential. But with it, your data will become the competitive edge that powers your future.

The AI revolution in the UK IT and telecoms channel

AI is revolutionising work in the unified communications sector, but with its transformative potential also come challenges, exploring the key areas where AI is making an impact, hurdles businesses must overcome and the opportunities that lie ahead for channel partners.

BY WILLIAM RUBIO, CALLTOWER'S CRO

AAI is reshaping several aspects of the UK IT and telecoms channel. Many companies are already using AI as a strategic tool to automate repetitive tasks like network monitoring, ticket management and fault detection. By freeing up time normally spent on tasks like these, agents are now able to focus on more value-driven initiatives or more complex issues.

AI-powered analytics tools are also enabling companies to make better data-driven decisions. Predictive analytics helps forecast trends, identify risks and create targeted business strategies. For instance, channel partners can now easily analyse customer behaviour to upsell or cross-sell more effectively.

And, arguably most importantly, virtual assistants and chatbots powered by AI are improving how businesses interact with customers- an incredibly important aspect of work in IT and telecoms. These tools provide 24/7 support, reduce response times and help resolve basic queries, leaving the more complex issues for agents to handle.

How companies can use AI to drive further success

When implemented thoughtfully, AI can provide significant advantages for performance, productivity, workforce engagement and customer satisfaction.

As mentioned previously, it can, and already is boosting productivity by automating routine tasks and reducing workloads, allowing employees to focus on strategic or creative tasks. But AI-enhanced workflows can also reduce common human errors and simple mistakes like misspelling, saving time and resources. Personalisation is another key area where AI shines and can be used more effectively for channel partners. Tools like recommendation

engines or personalised service portals ensure a better, tailored experience for customers, boosting customer satisfaction and retention.

Contrary to fears that AI replaces human workers, when used correctly, it can complement the workforce. AI can handle the exhaustive data processing that would take ages for employees to sift through, while employees can now take on roles requiring emotional intelligence or critical thinking, leading to a more engaged and satisfied workforce that is focussed on its strengths.

Challenges of implementing AI in the Channel

Though AI promises immense benefits, adoption in the UK IT and telecoms channel doesn't come without obstacles. Some of the common challenges our clients face are data accessibility and data quality, cost of adoption, skills gap and ethical and regulatory concerns.

AI systems thrive on high-quality data, but not all businesses have access to clean, structured and sufficient volumes of it. Poor data quality can lead to biased or unreliable outcomes. And the use of AI raises questions about data privacy and ethics. Misuse or mishandling of customer data can not only harm a company's reputation but also lead to regulatory penalties. And, implementing AI can be resource-intensive because of the upfront costs of integrating AI into their operations, including acquiring tools, talent and training. AI adoption requires a workforce skilled in data science and machine learning, where many organisations find themselves lacking employees with the technical expertise to manage AI solutions.

For businesses ready to tackle these challenges, AI opens doors to opportunity. By analysing customer data with AI, partners can identify customer pain points and offer relevant services, effectively turning insights into revenue opportunities

Opportunities for channel partners
For businesses ready to tackle these challenges, AI opens doors to opportunity.

By analysing customer data with AI, partners can identify customer pain points and offer relevant services, effectively turning insights into revenue opportunities. Channel partners can then build AI-driven solutions tailored to those specific customer needs. For instance, predictive maintenance tools for telecoms or cybersecurity services designed to protect against the latest threats.

The road ahead

Looking ahead, AI will likely evolve to play an even bigger role in the Channel. Some future applications include intelligent networks, hyper-personalised experiences, advanced predictive maintenance and sustainable solutions. With 5G adoption on the rise, AI will become integral to managing these complex and demanding networks.

By predicting equipment failures with even greater accuracy and alerting technicians before issues impact operations, AI could also minimise downtime in IT and telecom infrastructures. I think AI can also play a central role in reducing energy consumption in telecom infrastructures by dynamically allocating resources to optimise power usage.

AI has barely scratched the surface in delivering personalised services. Future applications may include context-aware customer interactions that anticipate needs before they arise.

AI is no longer just a buzzword; it's the engine driving transformation in the UK IT and telecoms channel. While challenges like cost, skills shortages and ethical questions exist, opportunities abound for those willing to adapt and innovate. By using AI as a strategic tool, businesses can create lasting value for both employees and customers. For channel partners, the key lies in recognising AI's potential, addressing existing gaps and exploring untapped markets. The future, guided by AI, promises to be both complex and exciting for the Channel.

MSP CHANNEL AWARDS 2025

CELEBRATING 15 YEARS OF SUCCESS

WE'RE PROUD TO HAVE LAUNCHED THE MSP CHANNEL AWARDS

INTRODUCING THE MSP CHANNEL AWARDS

A refreshed and rebranded evolution of the highly respected SDC Awards. This transformation reflects the growing influence of Managed Service Providers, who are now leading the way in delivering cutting-edge IT solutions across every industry.

We still have categories covering storage, backup, cybersecurity, and cloud infrastructure but we have added exciting new categories to better reflect the modern MSP ecosystem and the broader channel community — including vendors, distributors, resellers, and integrators.

Getting involved is easy and completely free. You can submit as many products or projects as you like — this is your opportunity to highlight your innovation, showcase your successes, and gain industry-wide recognition.

NOMINATIONS ARE NOW OPEN

KEY DATES:

5 SEPTEMBER	NOMINATIONS CLOSE
3 OCTOBER	SHORTLIST ANNOUNCED
6 OCTOBER	VOTING OPEN
7 NOVEMBER	VOTING CLOSES*
3 DECEMBER	AWARDS CEREWMONY

* Voting will close 17:30 GMT

Winners will be announced at a gala evening on 3 December 2025 at Leonardo Royal Hotel London City, London.

NOMINATE NOW!

mspchannelawards.com

T: +44(0)2476 718 970

Angel BUSINESS COMMUNICATIONS

SDC AWARDS

ANGEL EVENTS