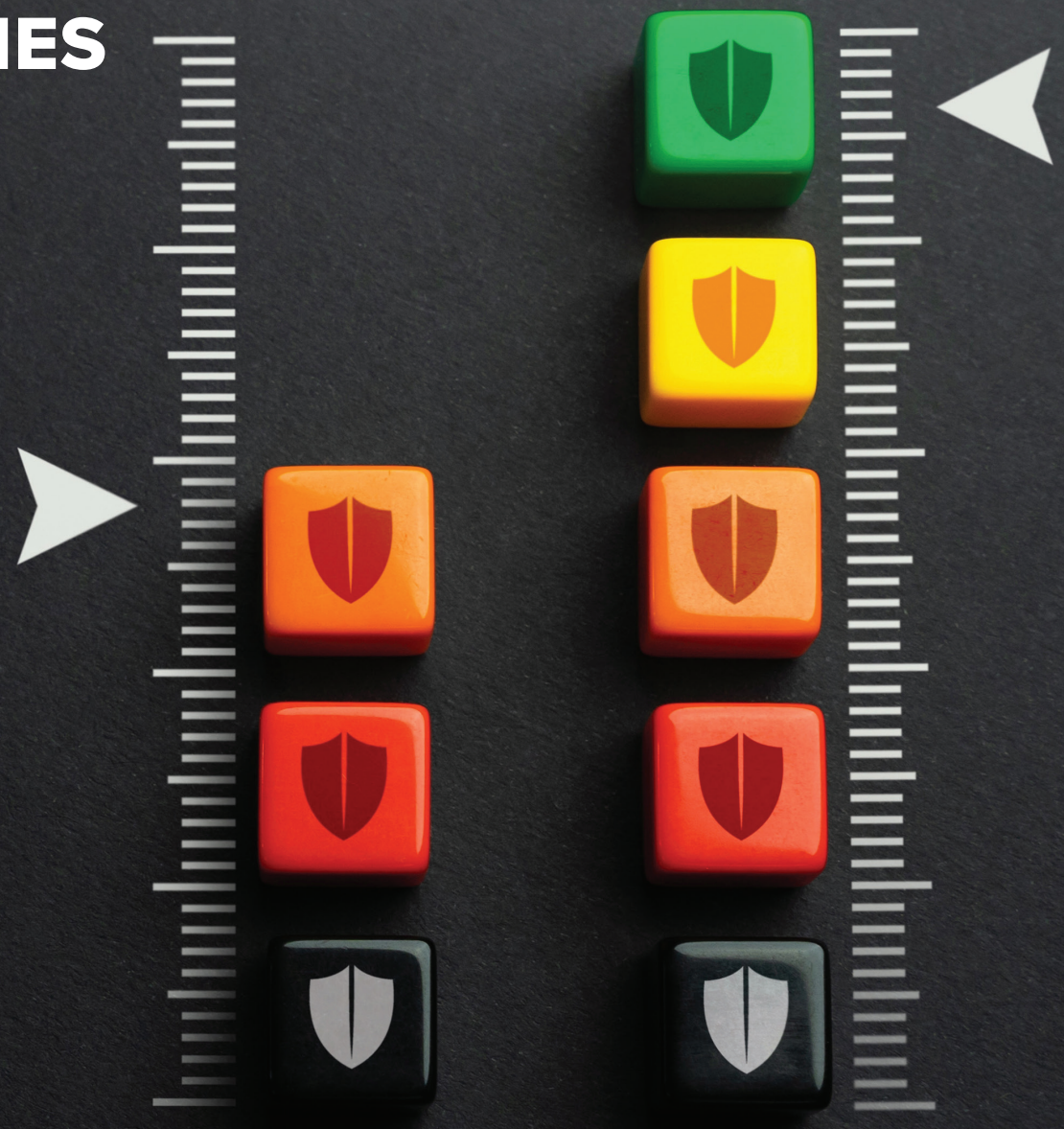
MSP CHANNEL INSIGHTS
CONNECTING THE CHANNEL PARTNER ECOSYSTEM
ISSUE VI 2025
AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION
MSP-CHANNEL.COM

CHANNEL PRIORITIES IN A SERVICE-LED ERA: FROM PRODUCTS TO OUTCOMES




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

VIEWPOINT

BY SOPHIE MILBURN
EDITOR

Navigating 2025's AI shifts and gearing up for 2026

I'M Sophie Milburn, the new editor of the MSP Channel Insights portfolio, and I'm genuinely thrilled to take on the role at a time of rapid change and innovation across the channel. I'm excited to join a publication with a reputation for clear, relevant industry insights, and I aim to keep that commitment at the centre of what we bring to our readers.

Over the coming months, I look forward to shining a spotlight on emerging MSPs and the innovators quietly reshaping the landscape. Interviews with industry leaders across the ecosystem will feature prominently, offering first-hand perspectives on the challenges, strategies, and opportunities defining this next phase of managed services. Events remain a cornerstone of how we gather insight. Being part of the MSP Channel Awards 2025, at the Leonardo Royal Hotel London City, reinforced how valuable these occasions are. The Awards evening gave the channel an opportunity to reflect on key milestones, recognise innovation, and spark strategic conversations that will influence the year ahead.

An industry lunch following the ceremony continued these discussions with senior executives, highlighting the key challenges MSPs faced in 2025. Among these, the rapid acceleration of AI, particularly in cybersecurity, stands out as the most pressing. AI is reshaping the threat landscape, enabling attackers to deploy automated, adaptive, and highly sophisticated methods that many providers have never encountered before. At the same time, persistent skills shortages, rising customer expectations, and the pressure to automate at scale are prompting MSPs to rethink how they operate and deliver value to their clients.

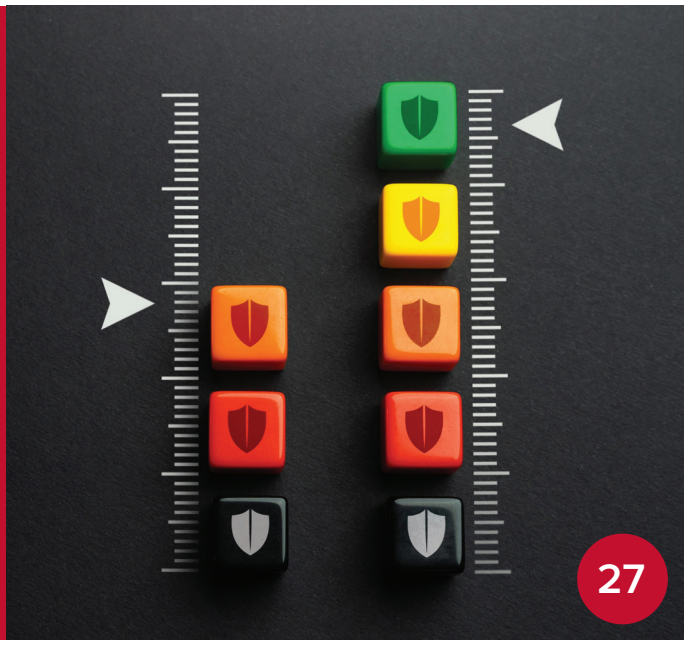
Yet, despite the trials of 2025, the outlook for 2026 remains one of opportunity and momentum. As we move into the new year, MSPs are expected to embrace AI not just defensively, but strategically, leveraging automation to streamline operations, enhance service delivery, and unlock new efficiencies. I'm particularly excited to continue these conversations at our Manchester 2026 roadshow, where leading industry voices will explore key themes shaping the channel, including cybersecurity and resilience in an AI-enhanced world, winning in a crowded MSP landscape, people, culture and leadership as differentiators, and strategies for growth, investment, and M&A.

By sharing these insights, I hope to highlight the strategies, ideas, and emerging voices that will define the months ahead. It is an exciting time for the channel, and I am committed to ensuring MSP Channel Insights remains a trusted guide as we navigate the opportunities and challenges of 2026 together.

COVER STORY

Channel priorities in a service-led era: from products to outcomes

The UK channel is undergoing a major transition. The traditional CapEx-driven approach, focused on product shipments and licence sales, is giving way to a service-first model. Customers now seek agility, resilience, and scalability, rather than a collection of disparate products



MSP CHANNEL INSIGHTS

Angel BUSINESS COMMUNICATIONS

Editor
Sophie Milburn
+44 (0)2476 718970
sophie.milburn@angelbc.com

Technology Editor
Philip Alsop
philip.alsop@angelbc.com

Business Development Manager
Aadil shah
+44 (0)7519 606 813
aadil.shah@angelbc.com

Senior Sales Executive
Graeme Davidson
+44 (0)2476 823124
graeme.davidson@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 eight 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)

Embedded AI: Beyond pilot phases

Trust in autonomous AI is rising, yet widespread adoption lags with UK leading in maturity.

NEW RESEARCH from Insight Enterprises highlights a growing trust in autonomous AI, as 57% of organisations report being 'very confident' in the technology's reliability within core business processes.

Despite this trust, implementation is slow, with six in ten organisations stuck in pilot or experimental phases. The majority employs AI in low-risk, narrow areas, with only 24% using it in production for defined use cases.

The UK demonstrates stronger AI maturity compared to its European counterparts, with 9% of organisations fully embedding AI into operations, topping the region, and ranking second in scaled deployments. Yet, the level of integration remains low, as 70% of UK businesses are yet to advance beyond small-scale pilots.

The Insight's EMEA AI Maturity Report suggests trust is not the issue, with just

1% of IT decision-makers doubting the technology. Instead, the delay in AI adoption stems from operational and organisational challenges:

- Technology integration issues (36%)
- Skills gaps for AI system management (23%)
- Cultural resistance (17%)
- Governance and compliance framework gaps (14%)

These challenges mean AI maturity remains limited, with most markets stuck in early or scaling phases. Only 5% of European organisations have AI fully embedded, while a further 15% have scaled AI production. This reveals a stark contrast between confidence and actual deployment.

Over half of the organisations (52%) prefer cloud-based AI, with 16% strongly supporting it. Nonetheless, 44% still opt for on-premises solutions due to concerns about control, compliance, and performance. Balancing cloud and on-premises workloads requires maturity that many enterprises have yet to achieve.

The survey captures the excitement surrounding AI's transformational potential but also notes the challenges in successful implementation. Limited results arise from a technology-led approach which merely places tools into teams without strategic integration.

As the leading AI Solutions Integrator, Insight suggests starting with business understanding, in collaboration with AI Forward Deployed Engineers.

Navigating AI compliance: A balancing act for UK IT decision makers

OVER HALF (51%) of UK IT Decision Makers (ITDMs) express uncertainty about the compliance of their AI-generated data with regulations such as GDPR. This revelation comes from a survey by Splunk, highlighting concern amidst the widespread adoption of AI in UK businesses.

Despite 88% of UK ITDMs engaging in AI projects, the potential repercussions of non-compliance, including hefty fines, linger as a threat. The survey, involving 500 ITDMs from sizable UK companies, also sheds light on future compliance concerns. A vast majority, 64%, anticipate increasing challenges over the next three years, compounded by 36% who have faced significant issues due to compliance failures.

Key Findings:

- The EU AI Act presents a major compliance challenge for 30% of respondents, despite its pending implementation, with significant implications for UK companies operating internationally.
- Over half (56%) report AI contributes to an 'unmanageable explosion' in data volumes, with 60% struggling to process and store this data.
- AI is cited by 33% as a main factor in 'runaway data growth', while 89% acknowledge a 50% increase in data volumes within three years.
- A lack of effective data management strategy affects 33% of businesses despite the surge in data volume.

Petra Jenner of Splunk highlights AI's enormous potential but underscores the complexities it brings, particularly in compliance and data governance. While 47% of ITDMs express confidence in their compliance efforts, a significant number remain skeptical, hinting at risks for businesses.

"The true differentiator for companies won't just be rapid AI adoption, but embedding trust, discipline, and compliance into their data strategies, ensuring safe and scalable integration." Jenner comments.

Ultimately, effective data management emerges as pivotal in bolstering AI's role in business, anchoring the upcoming generation of digital transformation while adhering to regulatory benchmarks.

Unlocking growth: The untapped potential of simplifying enterprise software

A new report reveals the hidden costs of software complexity in business, urging simplicity to enhance growth and efficiency.

AS BUSINESSES increasingly expand their technological frameworks, they face an insidious challenge: complexity. Freshworks Inc.'s latest report, The Cost of Complexity, meticulously quantifies this burden.

According to the study, which surveyed 700 professionals worldwide across various sectors such as IT, CX, finance, and operations, the ramifications are threefold: diminished revenue, impaired productivity, and eroded morale.

The report identifies that software itself is a massive contributor to this complexity, draining an average of 7% of annual revenue. This loss parallels typical R&D allocations, as noted by EY, emphasising its magnitude.

Businesses are wasting a significant 20% of their software budget on failed implementations and underutilised tools, costing the U.S. economy nearly $1 trillion annually.

- Over half (53%) of companies reported not achieving the planned ROI from software investments.
- A third (34%) cited revenue leakage from delays and missed opportunities.
- Many leaders (43%) experienced over-budget implementations in the past year.

Such inefficiencies stifle innovation, quietly sapping momentum until their effect cannot be ignored.

Research highlights that workers lose nearly seven hours weekly to convoluted processes and scattered tools, directly impinging on the bottom line.

- Workers manage an average of 15 software solutions and four communication channels daily.
- 45% report working in silos, with inadequate coordination across teams.
- 37% lack a centralised data source.

Such complexity hits CX and IT teams hardest, with frustrations around uncustomisable workflows, disparate tools, and outdated designs.

Complexity not only affects efficiency but significantly impacts morale. This concern is so pressing that 60% of employees are inclined to leave their jobs within a year due to these issues.

Drivers include:

- Organisational complexity (38%)
- Complicated processes (30%)
- Burnout and poor or difficult software (30% and 17% respectively)

When staff become disillusioned by complex systems, it not only affects retention but hinders mutual support and innovation.

To avoid treating complexity as an unavoidable cost, businesses must embrace simplicity, re-evaluate their technological stacks, and prioritise straightforward solutions. This strategic shift promises budget optimisation, recovers lost productivity, and elevates employee well-being, unlocking true growth potential.

Bridging the AI divide

Slalom's latest AI Insights Survey unveils disparities between executive AI enthusiasm and workforce readiness, highlighting crucial challenges ahead.

SLALOM, a leading business and technology consultancy, has shared early findings from its third AI Insights Survey, illustrating a significant difference in attitudes towards AI between executives and the workforce.

The survey, which included responses from 2,000 C-Suite leaders, delved into current and anticipated AI investment trends. While AI reigns supreme in corporate strategy, gaps in skills, systems, and leadership could impede progress.
Globally, nearly all surveyed companies anticipate increasing AI spending by

2026, advancing earlier predictions. Executives view these investments as balanced, yet a substantial 93% of organisations encounter workforce challenges, with half relying on legacy platforms for core applications.

The survey refers to AI's disruption as entering its "endgame," with executives like Amy Loftus, Slalom's Chief Customer Officer, predicting a complete AI-driven transformation by 2030.

The pivotal period for transition appears set between 2026 and 2028.

Sectors face misalignment between strategic AI initiatives and their practical execution. The drive towards increased AI implementation necessitates strong governance, workforce enhancement, and people-focused innovations. Amy Loftus emphasises the need for robust data foundations and frameworks to ensure trusted AI-led decisions.

Key Findings:

- **AI Investment Surge:** Nearly all companies forecast increased AI budgets in 2026, extending beyond 2025's expectations, with balanced integration with other priorities.
- **Cost Efficiency:** Reducing manual tasks remains the top investment impetus. Despite potential, only 38% witness AI providing higher-quality outputs, pointing to opportunities untapped.
- **Workforce Challenges:** Skill deficits are notable obstacles, with 93% of firms hindered, compounded by dependence on legacy systems.
- **Changing Skills Priorities:** A shift prioritises critical thinking over traditional human skills, with diminishing emphasis on communication and empathy.
- **Strategic AI Utilisation:** Two-thirds of organisations employ AI assistants for swift business needs, with 95% of executives comfortable in AI's strategic decision-making roles.

The survey indicates a rollout of AI confidence primarily driven by executives, while mid-tier leadership remains more cautious.

Executives depict measurable optimism, significantly favouring AI's positive impact on industry dynamics.

Slalom's research, conducted this year via GLG Insights, is poised to guide customers and executives in AI investment decisions, enhancing their strategic approaches amidst evolving AI landscapes.

The costs of legacy systems, multi-million loses

GLOBAL ENTERPRISEs are losing millions annually to outdated systems, highlighting an urgent need for modernisation.

The global enterprise landscape is fraught with the escalating costs of outdated systems, leading to substantial financial wastage. An insightful study by Pegasystems Inc., often branded as the Enterprise Transformation Company™, reveals startling statistics: approximately $370 million is lost annually across enterprises due to inefficiencies in modernising legacy systems.

A detailed survey conducted by Savanta involving over 500 IT decision-makers worldwide sheds light on these challenges. It was found that nearly $134 million is wasted annually on legacy transformation projects hindered by outdated methodologies.
This highlights one of the major contributors to financial losses stemming from technical debt.
The analysis noted other significant expenses, including $58 million spent on transformation initiatives that failed due to obsolete systems and $56 million on maintenance and integration.

The research also gathered opinions on technical debt management and dependency on legacy structures:

- Seventy-eight percent of respondents agreed that resources spent on older systems could be better allocated to projects enhancing business effectiveness.
- A significant number found removing legacy support too time-consuming and not prioritised by management.
- The dependence on legacy applications remains strong, with 63% relying extensively on outdated systems daily.

IT leaders overwhelmed by cyber recovery complexity

11:11 Systems unveils research revealing IT leaders' overconfidence amidst cyber threats, with Europe facing intense complexities and urgent need for improved recovery strategies.

11:11 SYSTEMS, a leading provider of managed infrastructure, has unveiled a revealing study concerning cyber threats and the preparedness of organisations. This comprehensive global study engaged over 800 senior IT leaders, detailing a worrying combination of overconfidence, complexity, and inadequate expertise, leaving businesses dangerously exposed to cyber threats.

Conducted across key regions such as North America, Europe, and Asia Pacific, the survey highlights that an alarming 81% of IT leaders perceive their organisations as overly assured in their recovery capabilities against cyber incidents. This belief persists even as they encounter escalating challenges—82% of those surveyed admitted to facing at least one cyberattack in the last year, and 57% experienced two or more.

Of significant concern is the perceived threat posed by AI, with 74% of respondents apprehensive that its integration could heighten their vulnerability to attacks. The concern is notably pronounced among European participants, who accounted for 48% of the study. Within Europe, the intricacies of planning emerged as a prevalent issue, with 40% of respondents marking it as a primary concern, especially prominent in the Netherlands and UK.

European entities report colossal financial ramifications from cyber-related downtimes. An astounding 78% documented losses up to $500K for just an hour of downtime, while 16% faced losses between $501K and $1M. A smaller, yet significant, 6% reported losses exceeding $1M. Recovery times compound such losses, with over half of respondents indicating recovery spans of one to two weeks, significantly impacting business operations and

incurring legal costs.

The research underscores a gap in leveraging cyber recovery providers, with only 17% of European businesses fully adopting these crucial services. Yet, over half prefer a hybrid approach, 21% manage recovery internally, and disturbingly, 8% have no strategy at all.

In a reflection of priorities, 25% of respondents recognise the pressing need for enhanced staff training and awareness, while 22% call for amplified investment in incident recovery solutions, matched by 20% emphasising the integration of resiliency and disaster recovery planning. A fifth suggests frequent testing and simulations, with 13% advocating for greater automation in recovery processes. Additionally, 59% of European respondents deem customisation of recovery solutions as extremely important, indicating a demand for tailored approaches.

Sean Tilley, Senior Director of Sales at 11:11 Systems shares, "This data confirms what we see every day... while it is positive to see that the majority are investing in cyber incident recovery, without the involvement of a specialist, these investments may not achieve the desired results."

Encouraging statistics reveal 97% of European respondents plan investments in cyber recovery over the next year, yet responses vary by country. While UK respondents experience fewer significant attacks, their concern is relative compared to experiences in France and the Netherlands, where higher instances of major incidents are recorded. The evolving landscape underscores the necessity for organisations to bolster strategies and safeguard against evolving threats.

The 2025 Cyber Resilience Report by 11:11 Systems was conducted with over 800 senior IT, security, and risk leaders globally. Its insights spotlight the growing burdens of cyber recovery planning, AI integration anxieties, and the spiralling cost implications of downtime.

Critical infrastructure faces new cyber challenges

A new report by Thales highlights mounting cybersecurity challenges faced by critical infrastructure in balancing innovation with resilience as AI and quantum advancements grow.

THALES, a global leader in technology and cybersecurity, has unveiled the findings of its 2025 *Data Threat Report: Critical Infrastructure Edition.* The report underscores the heightened cybersecurity risks confronting sectors such as energy, utilities, telecommunications, and transportation, as these industries navigate a rapidly evolving technological landscape.

Critical infrastructure providers are increasingly integrating advanced artificial intelligence (AI) systems to enhance operational efficiency and resilience. However, this trend is accompanied by new security challenges. The report highlights that 74% of organisations are investing in AI-specific security tools. Concerns remain substantial, with 64% worried about model integrity and 53% cautious about the reliability of third-party data sources. Quantum computing presents another formidable challenge.

The report reveals 58% of critical infrastructure respondents are experimenting with post-quantum cryptography to combat potential future decryption threats. Confidence in existing encryption methods is mixed, accentuating the need for regulatory guidance and robust safeguards to protect sensitive data.

An area of notable advancement is the reduction in breach rates. Only 15% of critical infrastructure organisations reported breaches in the previous year, a significant reduction from 37% in 2021. This improvement is attributed to the widespread adoption of multi-factor authentication, employed by 75% of organisations to secure employee access.

Despite these gains, operational risks persist, with misconfigurations, exploited vulnerabilities, and identity compromise posing ongoing challenges. Issues surrounding digital sovereignty also loom large. Over half of the critical infrastructure respondents indicated that compliance with mandates drove their data sovereignty efforts. However, only 2% have encrypted a significant proportion of their cloud-stored sensitive data, compared to a global average of 8%. The inconsistent use of discovery tools further complicates data security strategies, potentially impacting the protection of critical datasets.

The report illustrates a dual picture of progress and vulnerability. While breach rates have improved, the swift advances in AI and quantum technologies pose new security threats.

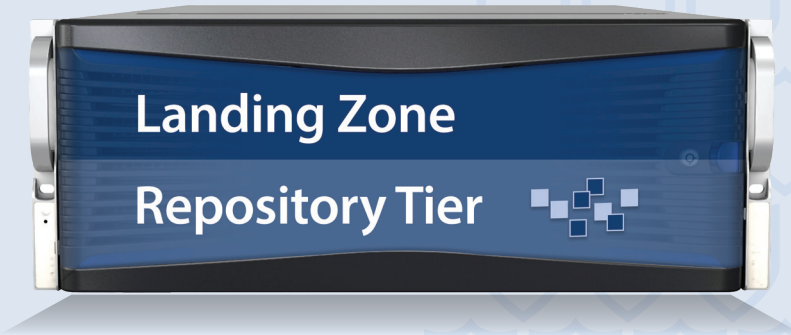
With rising regulatory scrutiny and geopolitical tensions, striking a balance between innovation and resilience is a priority. For critical infrastructure providers, proactive measures are paramount.

Investing in stronger encryption, AI-specific protections, and urgently preparing for post-quantum challenges will be crucial to safeguard sensitive data and maintain uninterrupted services.

Critical infrastructure providers are increasingly integrating advanced artificial intelligence (AI) systems to enhance operational efficiency and resilience. However, this trend is accompanied by new security challenges

EXAGRID®

The future is here.
Tiered Backup Storage



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

WINNER
SDC AWARDS 2024

- **Storage Company** of the Year
- **Storage Hardware Innovation** of the Year

Thank you so much to all who voted, and congratulations to our fellow SDC Awards 2024 winners!

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

LEARN MORE >

Gartner survey finds AI will touch all IT work by 2030

AI will touch all IT work by 2030, according to Gartner, Inc., a business and technology insights company. The IT estate of 2030 will be powered by humans, amplified by AI, and orchestrated by the CIO.

BY 2030, CIOs expect that 0% of IT work will be done by humans without AI, 75% will be done by humans augmented with AI, and 25% will be done by AI alone, according to a Gartner survey of over 700 CIOs conducted in July 2025. This means that organizations must balance AI readiness and human readiness to sustain value from AI.

During the opening keynote of Gartner IT Symposium/Xpo, which is taking place here through Thursday, Gartner analysts told the audience of over 6,500 CIOs and IT executives that few organizations are doing this.

"Gartner has been guiding CIOs and IT executives on their AI journeys for many years. In 2023, we showed them how to shape their AI ambition. Last year at IT Symposium/Xpo, we explained how to pace themselves in the AI outcomes race. This year, we're mapping out the right path for them to take so they can go all-in on AI value," said Gabriela Vogel, VP Analyst at Gartner.

"While not all AI is ready to deliver value, humans are even less ready to capture value," said Rob O'Donohue, VP Analyst at Gartner. "AI readiness means AI can help you find value and effectively meet the needs of specific use cases. Human readiness is about whether you have the right workforce and organization to capture and sustain AI value."

Transform the workforce to capture and sustain AI value

Gartner's position is that AI's impact on global jobs will be neutral through 2026. Gartner predicts that by 2028, AI will create more jobs than it destroys. "AI is not about job loss. It's about workforce

Gartner analysts Gabriela Vogel and Rob O'Donohue on stage at Gartner IT Symposium/Xpo in Barcelona.

transformation. CIOs should start transforming their workforces by restraining new hiring (especially for roles involving low-complexity tasks) and by repositioning talent to new business areas that generate revenue," said Vogel.

Restraining hiring will help to enhance productivity and optimize costs, but to capture new value, more needs to be done. The workforce needs to be able to work with AI in radically new ways. The skills they need are going to change.

"AI will make some skills, such as summarization, information retrieval and translation, less important, as AI is ready to automate or augment these tasks," said O'Donohue. "But AI also creates a need for entirely new skills. These AI skills are fundamentally different from most skills. Where skills were traditionally about doing tasks better, AI skills are about making you better — a better motivator, a better thinker and a better communicator."

Gartner analysts said organizations' skills development plans should go beyond training people in new skills. If people rely too much on AI and stop using their core skills, skills atrophy can happen. Workers should be tested periodically to make sure they are retaining critical skills for important roles.

Find AI value through AI readiness

AI readiness should be evaluated in terms of costs, technical capabilities, and vendors:

- **Costs:** In EMEA, 73% of CIOs reported that their organizations are breaking even or are losing money on their AI investments. For every AI tool organizations buy, they should anticipate 10 hidden costs plus the transition costs of training and change management. Organizations should conduct an analysis and decide which costs they'll fund.

- **Technical capabilities:** Some AI capabilities, such as search, content and code generation and summarization, are ready. Other capabilities, such as AI accuracy and AI agents, are not. When considering AI accuracy and AI agents, organizations should pivot from conversational agents to decision-making agents, and most importantly, they should invest in AI agents that are experts.

- **Vendors:** Determining the right vendor for an organization's AI needs is dependent on the type of AI implementation:
  - If an organization is planning a massive rollout of AI, hyperscalers have the AI infrastructure scale to support a wide range of outcomes.
  - For industry-specific use cases, start-ups can offer domain-specific AI agents, in-depth knowledge and capabilities that can deliver immediate benefits.
  - For rapid innovation and leading-edge AI capabilities, AI research and development companies are innovation-ready but don't quite have the raw scale to be fully enterprise-ready.
  - Every AI decision made is a sovereignty decision, so don't ignore AI sovereignty.

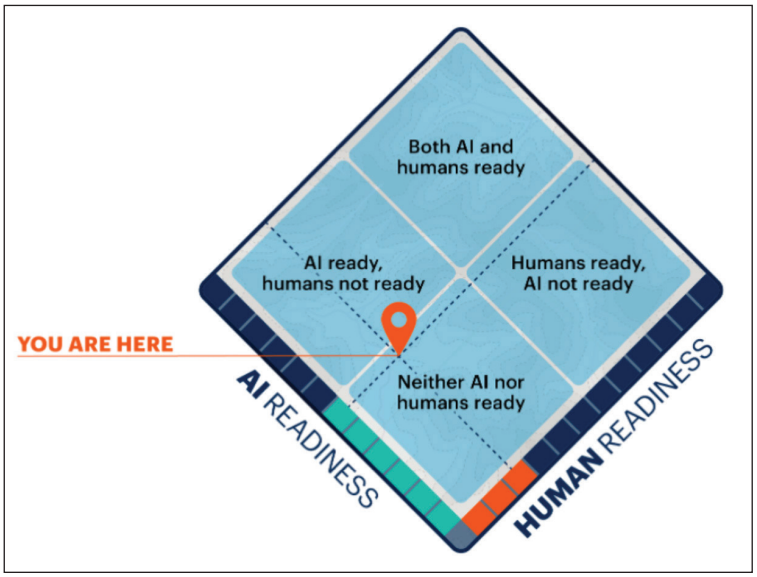


Figure 1: The "You Are Here" Gartner Positioning System (Example Position)

Gartner has identified four perspectives to assess how ready organizations are for every initiative they pursue. This system will help guide organizations on the path to AI value by gauging whether technology and human talent are ready to achieve their AI ambitions (see Figure 1).

"Following the Gartner Positioning System, organizations can seek to find, capture, and sustain AI value. If they are successful, they can transcend their limitations," said Vogel. "AI creates shockwaves which might turn a hospital into just a treatment center and might build an autonomous workforce for an autonomous business.

But the real payoff comes when AI solutions are focused on improving the core competencies of an organization or solving impossible problems." Gartner clients can learn more in "Walking the Golden Path to Value: 2025 IT Symposium/Xpo Keynote Highlights."

Gartner unveils top predictions for IT organizations and users in 2026 and beyond

Analysts Explore How AI Affects a World of Shattered Norms at Gartner IT Symposium/Xpo

Gartner, Inc., a business and technology insights company, today revealed its top strategic predictions for 2026 and beyond. Gartner's top predictions span three categories: talent in the AI age, sovereignty and insidious AI.

"The risks and opportunities of rapid technology change are increasingly affecting human behavior and choices," said Daryl Plummer, VP, Distinguished Analyst, Gartner Fellow and Chief of AI Research for the Gartner High Tech Leaders and Providers practice. "To properly prepare for the future, CIOs and executive leaders should prioritize behavioral

changes alongside technological changes as first-order priorities."

Gartner analysts presented the top 10 strategic predictions during Gartner IT Symposium/Xpo, taking place here through Thursday.

Through 2027, GenAI and AI agent use will create the first true challenge to mainstream productivity tools in 30 years, prompting a $58 billion market shakeup.

GenAI changes will allow organizations to prioritize requirements to GenAI innovations that accelerate work completion. Legacy formats and compatibility will decline in importance, reducing barriers to entry and resulting in new competition from a wide array of vendors.

The cost and packaging of everyday GenAI is likely to change over time, with vendors moving fee-based features into a no cost tier, potentially making no cost products suitable for more users.

By 2027, 75% of hiring processes will include certifications and testing for workplace AI proficiency during recruiting
Within the next two years, expect to see many organizations implementing practical AI proficiency assessments in their hiring processes. These standardized frameworks and targeted surveys allow companies to understand candidate proficiency and close gaps in AI skills within their workforce.

This trend will be especially pronounced for jobs where information capture, retention, and synthesis are major components.

As generative AI (GenAI) skills become increasingly correlated with salaries, motivated candidates will place a significantly higher premium on acquiring AI skills and need to demonstrate those abilities to solve problems, improve productivity, and make sound decisions.

Through 2026, atrophy of critical-thinking skills, due to GenAI use, will push 50% of the global organizations to require "AI-free" skills assessments
As enterprises expand their use of GenAI, hiring practices will begin to differentiate sharply between candidates who can think independently and those who lean too heavily on machine-generated output. Recruitment will increasingly emphasize the ability to demonstrate problem-solving, evidence evaluation and judgment without AI assistance.

This shift will lengthen hiring processes and intensify competition for talent with proven cognitive capabilities. In high-stakes industries, such as finance, healthcare, and law, the scarcity of such talent will raise acquisition costs and force companies to develop new sourcing and assessment strategies. Specialized testing methods and platforms designed to isolate human reasoning ability are likely to emerge, creating a secondary market for AI-free evaluation tools and services.

Enterprises that successfully integrate AI-free evaluation into their broader talent strategies will protect the "human edge" in decision quality and adaptability, providing an advantage that will compound as GenAI reshapes the competitive landscape.

By 2027, 35% of countries will be locked into region-specific AI platforms using proprietary contextual data
The AI landscape will fragment as technical and geopolitical factors force organizations to localize solutions, responding to strict regulations, linguistic diversity, and cultural alignment. Universal AI solutions will fade as regional differences grow.

Gartner analyst Daryl Plummer on stage at Gartner IT Symposium/Xpo.

Multinational companies will face complex challenges deploying uniform AI across global markets and will have to manage multiple platform partnerships, each with unique compliance and data governance demands. Buyers will prioritize regional platforms that offer strong performance and local compliance, while vendors will forge alliances with sovereign cloud providers and open-source models to remain competitive.

Global model vendors must prove their contextual value or risk losing market share, especially in regulated or culturally sensitive sectors.

By 2028, organizations that leverage multiagent AI for 80% of customer-facing business processes will dominate
A hybrid AI model, where customer relationship management (CRM) AI handles routine tasks and humans focus on complex, emotionally charged interactions, will become the industry standard. Moreover, customers will still choose between full self-service assisted by AI interactions such as performing a transaction or learning more about a product while also choosing a human, assisted by AI to help them with things such as resolving a complex situation or billing dispute.

Organizations that fail to adopt multiagent AI for their CRM organizational processes risk losing competitive advantage as customer expectations for low effort, rapid service become the norm. Moreover, customers who find low-effort experiences often stay with the supplier/brand because of the better experience.

By 2028, 90% of B2B buying will be AI agent intermediated, pushing over $15 trillion of B2B spend through AI agent exchanges

In this new ecosystem, verifiable operational data becomes a currency, fueling a data feed economy where digital trust frameworks and verifiability are prerequisites for participation. Products designed with composable microservices, API-first, cloud-native, headless architectures will establish a significant competitive moat. New commercial models will emerge, featuring high-frequency, frictionless sales powered by AI agents that can radically compress the sales cycle for a large range of business and technology purchases.

By the end of 2026, “death by AI” legal claims will exceed 2,000 due to insufficient AI risk guardrails Rising wrongful death incidents of AI-related safety failures, or “death by AI,” will lead to increased regulatory scrutiny and control, recalls, involvement of law enforcement agencies, and higher litigation costs.

As regulatory scrutiny intensifies, organizations will face pressure not only to meet minimum legal obligations but also to prioritize safety and transparency in their business systems through the use of AI guardrails. Somewhat paradoxically, companies will likely showcase either their AI use or lack thereof to differentiate themselves from competitors and mitigate the risk of potential litigation.

The impact of AI and decision governance failures will vary by geography due to differences in legal and regulatory systems, exposing organizations to varying risks and liabilities.

By 2030, 20% of monetary transactions will be programmable to include terms and conditions of use, to give AI agents economic agency
Programmable money is enabling new business models by allowing machine-to-machine negotiations, automated commerce, market discovery and data asset monetization, fundamentally reshaping industries such as supply chain management and financial services. Real-time programmable transactions deliver liquidity and efficiency gains by reducing friction, improving liquidity and lowering operational costs, which supports the rise of autonomous business operations.

The rise of machine customers, such as AI agents with economic agency, will increase demand for programmable financial infrastructure, create new markets, facilitate autonomous financing and enable products that automatically adapt to changing needs. As a result, stablecoins, deposit tokens and tokenized real-world assets are evolving into mainstream financial instruments for enterprise use.

However, fragmented standards and a lack of interoperability across programmable money platforms and blockchain infrastructures will inhibit market growth and prevent AI agents and machine customers from acting as true economic actors. Security vulnerabilities in programmable money storage, access control and transaction integrity will erode trust and prompt new regulatory frameworks to govern their use.

By 2027, the cost-to-value gap for process-centric service contracts will be reduced by at least 50% due to agentic AI reinvention
AI agents will evolve to discover tacit knowledge. and interactions with them will then become the process itself. Hidden knowledge utilized by these agents will lead to new value assets. Continuous innovation-based pricing will not be limited by labor as standardized workflows are replaced by context-driven orchestration.

By 2027, fragmented AI regulation will grow to cover 50% of the world’s economies, driving $5 billion in compliance investment
AI transformation is being built on AI governance. With more than 1,000 AI laws proposed last year, no two have a consistent definition of AI. AI governance can become an enabler or a barrier.

The channel's role in simplifying cloud complexity and reducing waste

Cloud computing is no longer just a buzzword – it is a crucial element of modern technology. Over the last few years, cloud services have integrated into our personal lives with an infinite array of applications and products available.

BY PETER OLLERENSHAW, CLOUD SOLUTIONS ADVISOR AT CYBIT

While Artificial Intelligence (AI) may dominate the current tech narrative, the hybrid cloud continues to gain momentum. Global adoption is projected to surge from $132B in 2025 to over $580B in 2034, with a compound annual growth rate of 17.63%.

Growing cloud complexity

As cloud usage expands, so does its complexity. Today's cloud environments resemble an intricate spider's web of interlinked, multifaceted, and interdependent services that are difficult to maintain or manage.

Symptoms of a challenging cloud ecosystem can manifest in several ways. Businesses frequently face configuration challenges, struggling to manage diverse platforms that each come with their own tools, interfaces, and settings. This places considerable strain on IT teams and increases the risk of misconfigurations. Recent reports also show that 32% of cloud spend is wasted, due to overprovisioning and lack of visibility. Without clear oversight, organisations can face unexpected expenses due to underutilised or untracked resources.

Security and compliance concerns also escalate as data and workloads span across multiple jurisdictions. Navigating regulatory requirements becomes increasingly complicated, and the rapid pace of cloud technologies demands specialist expertise. Many organisations lack internal resources to keep up, contributing to a widening skills gap.

Managed cloud services and FinOps

For channel partners, the challenge lies in helping customers regain control, reduce waste, and simplify operations. This is where FinOps comes in. As a strategic framework, it brings together finance, IT, and business teams to align cloud investments with business value.

When combined with managed cloud services, FinOps fosters a culture of accountability, transparency, and informed decision-making – all essential when navigating today's cloud landscape. This combination enables channel partners to deliver measurable impact by eliminating unused resources, optimising workloads, automating cost controls, and ensuring proactive monitoring, security reviews, and compliance checks.

Managed cloud services also relieve businesses of the burden of day-to-day cloud management. FinOps enhances this by enabling proactive resource tagging, which improves visibility and accountability, allowing issues to be resolved quickly so businesses can focus on what truly matters.

These services encompass infrastructure management, including provisioning, patching, and scaling to maintain optimal performance. They also provide real-time cost monitoring to help avoid budget overruns, and continuous performance optimisation through tagging to balance cost and efficiency.

In addition, AI-driven insights from vendors can be tailored to work with a company's own data to unlock strategic growth opportunities, accompanied by expert support that provides reliable cloud operations and peace of mind.

The importance of proactive monitoring

As cloud environments continue to grow in scale and complexity, the risks of security breaches, performance issues, and regulatory non-compliance also become more crucial. To maintain a secure and efficient cloud ecosystem, businesses need to deploy a proactive approach that includes monitoring, regular security reviews, and robust compliance checks.

Proactive monitoring uses real-time tools to track performance metrics, detect anomalies, and predict potential issues before they escalate. For example, a sudden spike in compute usage could indicate a misconfiguration or a security threat. With cyberattacks becoming more sophisticated and frequent, the stakes are even higher, with Sophos reporting that the average ransomware payment now exceeds $1M.

> Security and compliance concerns also escalate as data and workloads span across multiple jurisdictions. Navigating regulatory requirements becomes increasingly complicated, and the rapid pace of cloud technologies demands specialist expertise

Security reviews are equally critical. By routinely auditing cloud configurations, access controls, patching processes, and encryption protocols, businesses can stay ahead of threats by identifying vulnerabilities early and ensuring their environments remain resilient.

Finally, compliance checks like GDPR, FCA, and ISO 27001 impose strict requirements on data handling and security. Automated compliance tools help ensure that cloud environments adhere to legal and industry standards. Non-compliance can result in substantial fines or reputational damage, making regular checks non-negotiable.

Unlocking the full value of the cloud

The cloud offers immense opportunities for organisations, but its growing complexity demands strategic management. Whether an organisation is at the start of its cloud journey, or it needs to gain technical and financial control of its cloud estate, there is a solution available to secure their environment and optimise costs.

Channel solutions like FinOps drive cost efficiencies and foster accountability across teams, while proactive monitoring, regular security reviews, and compliance checks ensure a robust, secure cloud infrastructure. By partnering with the right providers and adopting disciplined practices, companies can fully harness the full potential of the cloud while remaining agile, secure, and cost-effective in a rapidly evolving landscape.

Enhancing supply chain security:

The strategic role of Managed Service Providers

Tim Grieveson, Chief Security Officer at ThingsRecon discusses the latest vulnerabilities affecting MSPs especially when a partnership is mismanaged.

IT MAY SOUND surprising, but no organisation truly owns its supply chain anymore. What was once a neat list of vendors now looks more like a tangled web of SaaS providers, cloud platforms, open-source dependencies, logistics partners, and fourth-party suppliers you've never even heard of. Each of those links is both an enabler of your business and a potential exposure point. The problem is, while the chain has grown more complex, the threats targeting it have grown sharper.

Consider the now infamous SolarWinds attack, which brought thousands of businesses and agencies to their knees, including the US government. Or the MOVEit incident, in which a zero-day vulnerability in a file transfer programme left businesses like British Airways and the BBC exposed to ransomware. The patterns here are the same: a single compromise or vulnerability cascades across hundreds or thousands of downstream organisations that had no knowledge of the risk until it was too late. It was a wake-up call for boards and executives who were met with an uncomfortable reality – traditional procurement checks and annual audits no longer measure up against the dynamic, real-time attack surface in which they find themselves.

This is where Managed Service Providers (MSPs) are having to step up. At their best, they act as an extension of the enterprise's security function, offering around-the-clock monitoring, standardised practices across fragmented ecosystems, and the ability to translate regulatory obligations into operational discipline. For mid-sized companies without the resources to build enterprise-grade security in-house, MSPs can provide access to the same expertise, tooling, and incident response capabilities that their larger peers rely on.

But while the case for MSPs is strong, the risk of over-reliance is equally real. Without proper oversight, transparency, and contractual clarity, the very partnerships designed to close security gaps can end up opening new ones. The challenge for leaders, then, is not whether to use MSPs - that decision is already being made across industries - but how to integrate them strategically into the governance of supply chain security.

Why MSPs are now more ‘partner’ than ‘provider’

In most organisations, the security team is already running at full stretch just trying to defend the perimeter. Expecting them to also map, monitor, and manage a sprawling web of third- and fourth-party dependencies is like throwing in some hurdles, pits, and a long jump at the end. It simply isn’t feasible. That’s why MSPs have had to evolve from peripheral providers to core partners.

Their value lies in reach and continuity: the ability to watch for threats that emerge at any point in the supply chain, not just within the walls of the enterprise. With 24/7 monitoring, dedicated threat intelligence, and scalable resources, MSPs can provide the kind of persistent vigilance that individual organisations would struggle to maintain on their own.

Just as important, MSPs bring consistency to an ecosystem that is anything but consistent. Every vendor, platform, and integration has its own security baseline, which means a business relying on dozens of suppliers is, in practice, inheriting dozens of different risk postures. By applying standardised controls and compliance frameworks, MSPs can smooth out those variations, reducing the weak spots that attackers so often exploit. It’s a technical win for boards, but it’s also a governance win. It translates a fragmented, opaque landscape into something measurable, reportable, and, most importantly, defensible in the face of tightening regulations.

MSPs might not have the power to eliminate the complexity of modern supply chains, but they do help ensure that complexity doesn’t automatically equal vulnerability.

A marker in the sand

A supply chain is only as strong as its weakest link, and in practice, that weak link is usually inconsistency. One vendor may follow strict patching cycles and compliance frameworks, while another cuts corners on updates or lacks visibility into its own subcontractors. Multiply that inconsistency across dozens or even hundreds of suppliers, and the result is a patchwork of exposures that no single organisation can realistically untangle. This is where MSPs add their magic. By introducing common baselines for monitoring, reporting, and compliance, they impose a degree of standardisation that individual organisations struggle to enforce on their own. The end result, when done well, is to bring discipline to a security ecosystem that is otherwise fractured and unpredictable.

Just as importantly, MSPs give enterprises the ability to respond faster when disruptions inevitably occur. A breach in a single supplier’s system can ripple outward with alarming speed, but MSP-led response frameworks can contain incidents before they escalate into wider crises. They also reduce duplication of effort; rather than every company in a supply chain reinventing its own protocols, MSPs can apply tested frameworks consistently across multiple tiers.

For those with a seat at the boardroom table, this consistency serves to extend visibility and resilience into places they cannot directly reach or influence. Put simply, MSPs act as force multipliers – a marker in the sand that amplifies security, response and continuity across the entire network.

From IT support to cyber guardian: why the MSP mindset must evolve

The nature of cyber risk is changing. UK businesses are no longer satisfied with one-off fixes and reactive cybersecurity. They want continuous risk management and monitoring.

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

THE GLOBAL managed security services market is booming. By one estimate, it's set to grow at a CAGR of more than 15% over the coming years to reach nearly $88bn (£66bn) by 20230. For end customers, investing in an MSSP is increasingly a no brainer, driven by cost, threat actor and skills pressures. For traditional managed service providers (MSPs), this is a huge opportunity.

But transitioning to become a fully fledged MSSP, or adding security to an existing portfolio of services, isn't without its risks. To get there, MSPs will need to choose their vendor partners carefully.

Why MSSP, and why now?

Trend Micro blocked 147 billion threats globally in 2024. That hints at the scale of the challenge facing UK organisations. In fact, government figures reveal that 43% of UK businesses suffered a breach last year, rising even higher for medium (70%) and large (75%) firms. As AI lowers the barriers to entry for opportunistic threat actors, boards are starting to appreciate the mounting impact on business risk. Yet a growing security workforce gap, which has reached 392,000 in Europe, and macroeconomic headwinds mean few have the resources to spend big on staff or security technology.

That makes managed security services an increasingly attractive option. That's especially true for businesses struggling to manage a growing number of compliance mandates, from DORA and NIS2 to the forthcoming UK Cyber Security and Resilience Bill.

As their digital footprint grows, as it must, so does their attack surface and the potential impact of a security breach. Insurers are also demanding investments in services like managed detection and response (MDR) in order to qualify for coverage or lower premiums.

All of which should be music to the ears of ambitious MSPs. Those prepared to evolve into an MSSP could benefit from increased margins, new revenue streams, competitive differentiation, and increased customer loyalty. But if it were that simple, every MSP would be doing it. The truth is that many providers are also struggling with skills shortages, and economic and business uncertainty that tends to stymie major transformation initiatives. They're

also keenly aware that this is already a highly competitive space where reputation is hard won and easily lost. This is where choosing the right vendor becomes critical.

The platform play

MSPs should do their due diligence carefully. The market is full of vendors all touting silver bullet, AI-powered solutions to everything from GDPR compliance to employee fraud. Peer reviews and independent assessments by analyst houses are a good way to whittle these down. The right vendor will also have well-regarded enablement, training and go-to-market programmes to help MSPs close skills gaps and resource shortages.

Even more important are platform-based offerings which centralise multiple capabilities in a single, multi-tenancy solution. This reduces complexity and administrative overheads for the MSSP/MSP, while keeping end-customer data secure and isolated and supporting more seamless, cost-effective scaling. Look for vendors that offer a broad range of threat prevention, protection, detection and response capabilities across multiple layers of the IT environment. This means threats can be more effectively correlated from different parts of the platform for improved insight and response.

A strong vendor focus on automation and AI can also help to take more of the pressure off the partner's in-house team, streamline workflows and reduce alert overload. Generative AI assistants are particularly useful in helping to act as security operations "copilots". Better still, find a vendor offering MDR services, where their expert team does most of the heavy lifting.

Embracing the change

So how can ambitious MSPs embrace these trends and evolve their services? This first step must be assessing their current offerings and skill sets and identifying any gaps in capability. They will need to build a business case for any transition, focusing efforts on a clearly defined target market for maximum impact. Then it's time to do that vendor due diligence. Investment in technology and skills are unavoidable, but they don't have to be prohibitive

Some channel programs in Europe are already embracing the shifting landscape. For example, one global cybersecurity vendor recently overhauled its partner program to reflect the new reality, removing the distinction between MSP and MSSP and replacing it with a unified programme.
Time to grow

The nature of cyber risk is changing. UK businesses are no longer satisfied with one-off fixes and reactive cybersecurity. They want continuous risk management and monitoring.

They want to understand their threat exposure in real time, and they need partners who can help them interpret that information and continuously remediate any issues to build resilience. MSPs that can deliver on these requirements will be well placed to differentiate themselves.

They could also be on a fast-track to growth. Canalys estimates annual channel revenue growth was just 5% in 2024, while that for managed security services hit 15%. Those are figures no MSP can ignore.

How speed to market shapes distribution success

In distribution, timing is crucial. It's not just a question of how fast a vendor gets to market - it's timing which determines whether they break through at all. Decisions about when and how a product launches influence its visibility, positioning, and how quickly the right partners can start building a pipeline. Even the best technology in the world will falter without the right velocity behind it.

BY TIM POPOVICH, COO, CLIMB CHANNEL SOLUTIONS

EMERGING VENDORS are moving at pace. Partners are evolving to meet new demands. However, the distribution model often struggles to keep pace. The real question isn't whether speed matters, because we know it does, but whether the channel is equipped to move quickly in ways that are meaningful, scalable, and built on genuine relationships.

What that demands is not just more automation or more tools. Instead, we need to rethink what effective distribution looks like in practice.

Rethinking speed

Speed in distribution isn't just a single metric. It's not only about processing quotes faster or onboarding vendors more quickly, though those are certainly important aspects.

At its core, it's about responsiveness: the ability to act decisively when an opportunity presents itself, to move in sync with partners, and to quickly align on what needs to happen next.

This kind of responsiveness is built through proximity and personalization. It's about knowing who to speak to, having direct access to decision-makers, and working with people who understand your business, not just your deal size or tier status.

Despite all the talk about digitization, distribution remains a relationship-driven business. What sets high-performing distributors apart is their ability to pair fast execution with the confidence that comes from deep familiarity with the channel and the people who drive it.

Supporting emerging technology with urgency and focus

For many new vendors, the clock starts ticking the moment funding is secured. Investors expect growth, and founders expect scale. What they don't have time for is a long, drawn-out onboarding process or a rigid go-to-market (GTM) strategy that assumes market traction will materialize on its own.

Early-stage vendors are often launching into noisy markets with limited runway.

They need distributors who can move quickly to validate demand, mobilize resellers, and get the message out to the right audience.

Experienced distributors understand that momentum compounds. The sooner a product is visible to the right partners, the sooner those important conversations can be had, the sooner that pipeline starts building, and the sooner revenue starts to build. All of this is easier to achieve when the process is structured, responsive, and tailored to the vendor's specific strengths and go-to-market needs.

In a sense, you can think of this distribution model like a well-oiled machine that works because the fundamentals—strategy, communication, alignment—are in place and the right people are there to keep it running effectively.

People still power the channel

It's this human element that often gets overlooked in conversations about distribution performance. But it's critical. It's the result of years–even decades–of investment in understanding how partners operate, what they need to succeed, and where new solutions fit. The most effective distributors have built their value by acting as trusted advisors to the reseller community. And when a vendor needs to move fast, that long-established trust and recognition make it possible to hit the ground running.

That same principle applies on the partner side. Resellers need to know that when a deal is on the line, the distributor is ready to respond clearly and without delay. The ability to get a quote turned around in hours, not days, isn't just a nice-to-have.

The strongest distributor relationships are built on reliability. When a partner sends up the signal that they're ready to get moving, they need to know someone's there to catch it.

And this isn't limited to order processing. Consider renewals: for many vendors, they're a key source of recurring revenue, but only if they're tracked, managed, and quoted at the right time.

A distributor who treats this as a passive admin task will leave money on the table. One who understands it as a strategic moment of customer engagement can drive both retention and upsell. Again, it's not just about raw speed. It's about having people in place who understand what the customer needs and who are equipped to deliver it, quickly.

Systems and data matter, not as a commodity, but as a way to deliver real value. The best distribution teams use analytics to spot where interest is building, which partners are leaning in, and what's likely to gain traction next. Crucially, they share that insight. By passing it on to vendors and resellers, they help shape smarter positioning, sharper targeting, and more effective marketing. It's not just about what the data shows, but how quickly and transparently it's used to support growth on both sides of the channel.

For emerging vendors, this kind of responsiveness is immensely valuable. Their margin for error is narrower and their cycles are shorter. If a product hasn't gained meaningful traction within the first 12 months, it can signal deeper challenges ahead. Which is why every launch, every introduction, and every conversation with a partner matters. Speed gives those interactions weight, and gives vendors the best possible chance of turning early promise into long-term growth.

The new competitive edge in distribution isn't found in broader catalogs or longer line cards. It's found in depth: in how well a distributor understands the needs of the vendors they onboard, the partners they serve, and the end users they ultimately reach. It's found in the ability to connect those dots in real time and to keep connecting them as markets shift and technologies evolve.

None of this is flashy, but it is essential. Distribution may not always get the headlines, but it makes the difference between an emerging idea and a rising vendor star.

The distributors who understand this don't just talk about speed as a vague idea, they live it by designing everything they do to reduce lag, eliminate guesswork, and create space for partners to sell effectively.

Because when the right people are empowered to operate at speed, they don't just move mountains...they move markets.

Simplifying cybersecurity: how MSPs can support their customers

Organisations today face mounting challenges in securing their networks, applications, and sensitive data. Attackers are now using generative AI to automate and scale their efforts, increasing the sophistication and volume of attacks. The availability of “as-a-service” tools further lowers the barrier to entry for cybercriminals.

BY ANDY COCKING, SALES DIRECTOR, MSP, EMEA & APAC, BARRACUDA

TO PROTECT against new and escalating threats, many organisations are acquiring an ever-growing stack of security tools. Managing these disparate tools – often from different vendors – creates a further drain on the internal IT team’s time and resources.

The need for support from partners in managing this complexity was one of the key findings in our MSP Customer Insight Report 2025. This explored the challenges facing organisations, what they need from partners and how MSPs can evolve – through their own skills and service offerings - to support their customers’ growing requirements in building cyber resilience.

The demand for MSPs’ security services

Protecting an organisation from cyber threats requires a combination of tools and expertise. Organisations need around-the-clock monitoring, management and mitigation capabilities, as well as a deep understanding of the threat landscape.

The reality is that few organisations can meet all these needs in house. As such, we found that the majority of organisations surveyed, 73%, outsource security services to an MSP and a further 18% are currently evaluating providers.

The research also highlights the importance of partners as organisations grow. As IT environments expand, internal teams often struggle to maintain the same level of visibility and rapid response needed to stay ahead of evolving threats, making outside expertise increasingly valuable.

We found that 52% of the organisations surveyed want MSPs to help them

CHANNEL INSIGHTS 2026 ROADSHOW

Hyatt Regency Manchester
55 Booth St W
Manchester
M15 6PQ

Manchester, UK

27 January 2026

MSP CHANNEL INSIGHTS ROADSHOW

REGISTER NOW

Now entering its **second year**, the **MSP Channel Insights Roadshow** returns with an expanded programme and evolved agenda – **connecting forward-thinking MSPs and IT service providers** with industry experts and carefully selected technology partners.

Manchester has firmly established itself as one of the **UK's leading digital and tech hubs**, known for its rich industrial heritage, vibrant innovation scene, and a thriving community of technology-driven businesses.

With a strong regional infrastructure, access to top-tier universities, and a **rapidly growing base of MSPs**, **cybersecurity firms**, and **cloud providers**, Manchester offers fertile ground for collaboration, innovation, and growth within the managed services sector.

As a **centre of excellence** for digital transformation in the North of England, Manchester provides a **strategic platform** for MSPs to engage with industry peers, explore evolving client needs, and stay ahead of trends in cybersecurity, AI, and IT service delivery.

Delegates will gain access to **expert-led fireside chats**, **panel sessions**, and **private boardroom discussions**, designed to tackle **real-world** challenges and provide actionable strategies for sustainable MSP growth. Topics for **2026** include cybersecurity, investment and M&A, smarter sales and marketing, and a new focus on leadership, culture, and talent – **all explored through the lens of innovation and AI adoption**.

Apply for your place today, limited to 30 industry experts per event.

msp-roadshow.com/events/manchester-2026

SCAN ME

The demand for cybersecurity support is growing across all business sizes. We are seeing ever larger organisations seeking the assistance of MSPs to help them with specific IT security challenges

manage a growing number of disconnected security tools and vendors, and 51% turn to MSPs to evolve their security strategies as the business expands.

For partners that can support customers with this growth there are clear commercial opportunities. The vast majority of respondents, 92%, are willing to pay more for support with security tool integration, which underlines the high value placed on managing this complexity.

The expanding customer base

The demand for cybersecurity support is growing across all business sizes. We are seeing ever larger organisations seeking the assistance of MSPs to help them with specific IT security challenges. This may reflect the growing scale and sophistication of security stacks in larger organisations, which require greater expertise and oversight from IT teams.

The larger organisations surveyed were more concerned than smaller ones about the growing complexity of their security environment (42%) and the growing complexity of cyberattacks (46%). These concerns highlight that the demand for MSPs services is extending well beyond their traditional SMB customer base. It's not only the customer base that is widening: the expectations from customers of the cyber security services they need from partners is also growing.

Strategic partners

MSPs are being viewed not just as service providers for technical delivery, but also as strategic partners that can help enterprises navigate and manage the escalating demands of cybersecurity operations.

As security and regulatory demands multiply, customers are looking for providers who can deliver a wider range of capabilities, such as incident recovery, regulatory compliance support and proactive resilience planning. They need forward-looking security advice as well as strategic security insight that scales with their own business growth and emerging threats.

Many are also turning to MSPs for expertise in next-generation capabilities such as Zero Trust, secure access service edge (SASE), and artificial intelligence (AI). For example, we found that 39% of organisations expect to need MSP support with AI and machine learning in the next two years.

What this means for MSPs

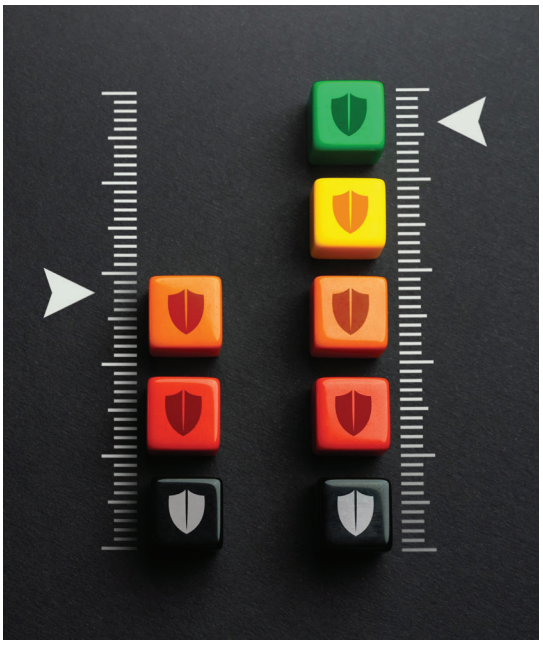
The findings reveal that organisations of all sizes now depend on MSPs for their security expertise and managed solutions. And as demand for advanced technologies and security continues to rise, MSPs will remain central to the success, resilience, and growth of businesses worldwide.

To capitalise on these opportunities, MSPs must expand their expertise and evolve into strategic security partners. In the coming years, they must strengthen their own operations - from talent and expertise to risk resilience - while continuing to meet evolving customer needs in an increasingly challenging cybersecurity landscape. At the same time, providers face their own challenges managing multiple clients whilst keeping pace with these new threats.

This is where vendors can support, through simplifying how MSPs manage their own IT environments: integrating management, response, and reporting through centralised dashboards and product consolidation. Working with vendors, with managed SOC capabilities can also reduce the burden on delivering 24/7 monitoring and response, enabling MSPs to focus on strategy, innovation, and building their customer relationships.

MSPs must expand their expertise and evolve into strategic security partners. In the coming years, they must strengthen their own operations - from talent and expertise to risk resilience

Channel priorities in a service-led era: from products to outcomes



The UK channel is undergoing a major transition. The traditional CapEx-driven approach, focused on product shipments and licence sales, is giving way to a service-first model. Customers now seek agility, resilience, and scalability, rather than a collection of disparate products.

BY JOHNNY CARPENTER, VP CHANNELS AND ALLIANCES EMEA AT 11:11 SYSTEMS

FOR PARTNERS, this shift requires more than a new business model. They must assess sales processes, address gaps in problem-solving, and train teams to prioritise customer outcomes over transactions. Adapting to this model is essential for continued relevance.

Service neutrality redefines the rules

Compensation is the first area of change. Traditional incentives favoured CapEx-driven, one-time sales. Now, leading partners are revising incentive structures and working with stakeholders to introduce service-neutral rewards that align seller incentives with customer preferences, whether OpEx, on-prem CapEx, or hybrid models.

This change enables sales teams to prioritise the best solutions for customers, not just the most profitable ones. It represents a cultural reset, placing trust and long-term value at the core of partner–customer relationships. The priority is clear: align incentives with customer outcomes. By linking compensation to customer success metrics instead of product preferences, partners can build credibility and foster strategic relationships. This approach enhances transparency and positions partners as trusted advisors in a trust-driven market.

Cyber resiliency moves centre stage

Given the recent spate of cyber attacks, resiliency has become non-negotiable. Customers no longer see security, backup, disaster recovery, and compliance as disconnected categories. They see them as inseparable pillars of business continuity.

But delivering that in practice isn't straightforward. Partners should map required technology integrations, vet potential providers, and design unified processes and service agreements that provide customers with comprehensive, reliable, and easy-to-consume solutions. Resiliency must now be embedded into every service offering. Customers increasingly expect security, recovery, and compliance to be delivered as a unified outcome, and partners must rethink how these elements are packaged and managed. Ultimately, resiliency becomes a value proposition that differentiates partners who can deliver peace of mind alongside performance. Cyber resiliency delivered as a managed, outcome-based service is fast becoming table stakes. Those who can offer it as part of an integrated portfolio will not just add value, but become indispensable.

The complexity challenge

The biggest pressure point facing IT teams is integration. They want simplicity, but solutions often deliver complexity. Partners must bridge this gap.Our latest global study of more than 800 senior IT leaders reveals that most are grappling with increasing complexity in cyber recovery planning. Partners must step in to simplify this challenge, not with a single silver-bullet solution, but by orchestrating multiple offerings into a seamless, unified experience that eliminates complexity for customers.

This is where simplicity becomes a competitive advantage. Customers are less interested in the underlying architecture and more focused on seamless experiences. Whether it's connecting cloud platforms, streamlining data flows, or harmonising user interfaces, the ability to simplify complexity is what will set partners apart.

In this environment, the role of the partner evolves from implementer to orchestrator, curating ecosystems that work together effortlessly to drive business value. Success isn't about controlling every element or owning every product; it's about creating the optimal mix, managing interoperability, and being accountable for the results. That's how trust is built, and trust is what today's customers value most.

The next phase

The way forward isn't about abandoning CapEx models altogether. It's about balance. The channel of the future is defined by flexibility, neutrality, and above all, outcomes.

For partners, the opportunity is as significant as the challenge. Those who evolve quickly by integrating services, rethinking incentives, embedding resiliency, and building trust through simplicity will set the pace in this service-first era.

Automatic remediation for complete data protection

How AI-driven automation helps Managed Service Providers eliminate risk from phishing and data loss before it spreads

BY JAMES GRIFFIN, CEO OF CYBERSENTRIQ

DATA is not unbreakable and keeping it protected across every client environment has never been more complex. For Managed Service Providers (MSPs) balancing multiple infrastructures and users, the scale of information entering networks each day makes it challenging to maintain visibility.

Threat actors know this and exploit the cracks that appear when human monitoring and manual processes are stretched too thin.

Email remains a particularly rich target. Despite improved filters and user awareness training, social engineering still succeeds.

Attackers craft convincing messages that prompt users to click links or open attachments that deliver malware or ransomware. Within minutes, data can be encrypted, credentials stolen and operations disrupted. The longer remediation takes, the greater the potential damage.

The limits of manual remediation
Traditional remediation models depend on manual investigation and cleanup. A security team might isolate compromised files, analyse the root cause and then roll out fixes across the environment. While this approach may have worked in simpler infrastructures, it is now too slow and too reactive.

Automatic remediation changes this equation. By applying artificial intelligence and automation to data protection, MSPs can respond to threats the moment they arise. The technology scans, identifies and isolates malicious content in real time before it ever reaches the user's inbox. The attack is contained before damage occurs, eliminating the gap between detection and response.

Manual remediation is no longer fast enough to match the speed of modern threats. By combining AI and automation, MSPs can protect client data instantly rather than after the fact, reducing both the impact and the workload on their teams.
As phishing and ransomware techniques evolve daily, speed has become the decisive factor in maintaining client confidence and business continuity.

How automation strengthens defence
Automatic remediation also closes the most persistent vulnerability in cybersecurity, human error. Even with training, no employee can detect every phishing attempt. Attackers continually refine their tactics, often impersonating trusted contacts or suppliers.

Automation removes that uncertainty by acting before a user can make a mistake.

This proactive approach eases the strain on security teams. MSPs already manage high alert volumes, compliance requirements and client expectations. By automating repetitive investigation and cleanup tasks, engineers can focus on strategic work such as threat hunting, policy refinement and resilience planning. Automation does not replace human expertise; it enhances it by dramatically increasing speed to action across defence, removing repetitive and error-prone elements of defence.

Cloud-based cybersecurity platforms extend this advantage by offering a single unified layer of protection across every managed tenant. Suspicious files or emails are quarantined automatically with alerts sent directly to administrators. MSPs gain visibility across their clients' networks without juggling multiple disjointed tools. Dangerous data is neutralised instantly and all actions are logged for audit and compliance.

As cyberattacks grow more targeted, clients increasingly look to MSPs as trusted partners rather than service providers. Delivering seamless, always-on protection demonstrates foresight and reliability. It builds long-term trust and positions the MSP as a guardian of client resilience.

Building resilience through unified protection

The benefits of automation extend beyond immediate threat containment. By integrating automatic remediation into their broader data protection strategy, MSPs can ensure consistency across backup, recovery and compliance. Cloud infrastructure allows them to scale protection easily in line with client growth.

> As phishing and ransomware techniques evolve daily, speed has become the decisive factor in maintaining client confidence and business continuity

Artificial intelligence continues to evolve, bringing new levels of precision to remediation. As AI learns from each attempted attack, it strengthens pattern recognition, reduces false positives and helps anticipate emerging threats. This continuous improvement gives MSPs an advantage that manual systems can never achieve.

In a landscape where data volumes are expanding and attack speeds are accelerating, delay is no longer an option. Automation reduces response time to zero and provides assurance that information across all environments remains protected, even as new threats appear.

Complete data protection cannot be achieved through disconnected tools. It requires an intelligent automated system that sees and responds to everything in real time. Automatic remediation delivers that capability, turning reactive defence into continuous resilience.

A smarter path to total resilience

For MSPs, adopting automatic remediation is both a competitive advantage and a strategic necessity.

As the threat landscape continues to grow more dynamic and clients increasingly expect immediate protection, automation becomes essential.

By integrating automation into their data protection frameworks, MSPs can deliver consistent assurance, faster response times, and measurable value across every customer relationship.

Automation also enables profitable growth. As service portfolios expand and new clients are onboarded, remediation processes that rely solely on people reach a breaking point. AI-driven remediation scales instantly without adding headcount or administrative overhead, keeping protection aligned with business growth.

The organisations that act now will set the benchmark for best practice in cybersecurity. They will respond to incidents before disruption occurs, demonstrate compliance without delay and deliver the confidence clients expect from a modern managed service.

Automatic remediation is no longer an optional enhancement. It is the foundation of complete data protection and the key to lasting trust between MSPs and the businesses they serve.

Those who lead on automation today will define the standard for resilience tomorrow.

Reigning in the mobile device frontier:

The Wild West of the digital workplace

With hybrid work models adopted by many companies in recent years, more than ever, IT teams are required to ensure that team members can work safely and securely on the remote endpoints of their choosing – including their own personal devices under a bring-your-own-device (BYOD) policy.

BY JASON BAYTON, ANDROID ENTERPRISE EXPERT AND PRODUCT LEAD AT NINJAONE

UNMANAGED mobile devices can significantly increase an organisation's attack surface and limit employee productivity because of outdated software, unsecured networks, potentially harmful applications, or compatibility issues. With so much work increasingly being done at the endpoint, lost devices, phishing attacks, and app-borne malware are just a few ways poor endpoint management practices can compromise modern enterprises.

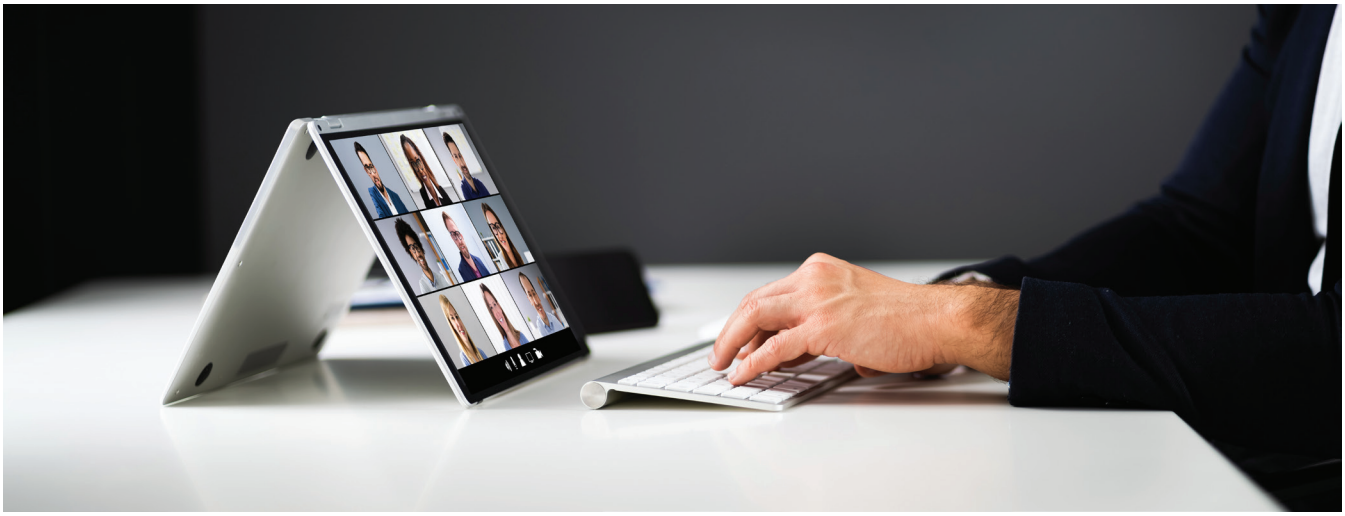
Seventy percent of employees are now using four or more endpoint devices per day, and a recent survey found that almost half (39%) of organisations have experienced a data security breach due to a lost or stolen device. Enterprises continue to find themselves facing an increased attack surface and, as a result, grappling with heightened risks. Much remains in flux as the attack surface continues to heat up and AI-enabled threats emerge on the scene – and this unique variety of challenges doesn't show any signs of slowing soon.

As CISOs and security teams struggle to balance individual device preferences and enablement with effective endpoint management and security at scale, here's where a consolidated approach to mobile device management (MDM) can help strengthen organisational resolve while enabling a more productive, efficient, and resilient digital workforce.

More flexibility for employees, more complexity for IT

Most IT networks today effectively support personal and company-owned mobile devices including phones, laptops, and tablets – as lines between personal and business device usage blurs. As a result, a wide array of operating systems and devices connecting from more locations is forcing IT teams and CISOs to address the rising risk of tech sprawl within their organisation.

Shadow IT, where employees use devices and applications without IT or security knowing about them, remains a persistent threat. According to IBM, over one-third (38%) of employees acknowledge sharing sensitive work information with AI tools without their employers' permission. When considering the range of freely accessible apps and services available on unrestricted app stores, and the ability to side-load applications outside of these, IT teams have an even broader bevy of novel risks to contend with. Without controls,



unauthorised apps can steal data or introduce malware, placing enterprises at risk. Even perfectly viable third-party applications can introduce data loss protection concerns. With so much at stake, visibility is essential to scale endpoint operations while staying ahead of risk.

Where MDM makes the difference

CISOs are finding it increasingly necessary to have access to tools that can provide better insight into employees' use of authorised (and unauthorised) tools. This can be achieved through endpoint monitoring and management systems, which increase visibility over all devices and applications and enable automated patching and secure cloud-first backups. Automated discovery tools can also work to identify unsanctioned software and enforce security policies.

Another core technical component that can assist CISOs and security teams in achieving this balance between device enablement and security is an MDM solution. MDM solutions can offer CISOs and bootstrapped security teams a standardised method of managing mobile devices at scale. MDM platforms can provide a single interface where IT administrators can enrol and monitor mobile devices, create and enforce mobile device policies, and set restrictions to deliver a consistent, familiar user experience, while protecting the organisation against threats posed by unmanaged devices.

Better policy enforcement means stronger device security and minimised risk, while still ensuring employees can do their best work from the devices of their choice. To this end, MDM solutions

are incredibly effective in helping organisation tackle compliance-related challenges as well.

But with the threat landscape growing and evolving so rapidly, and people remaining top targets in increasingly persistent attacks, it's not just solutions that CISOs and security teams need to employ to curb risk. Comprehensive security awareness trainings – continuously updating personnel on the latest adversarial tactics and educating them on the security implications of their actions – are just as essential.

Every employee should understand the risks of sideloading applications, granting overreaching permissions to untrusted applications, clicking links or engaging with unknown correspondence, or using untrusted Wi-Fi networks. They should also be aware of their organisation's escalation paths for reporting suspicious contact, and what to do if they lose a device. The faster an IT team is notified of a device that is lost or stolen, the faster they can lock it down or wipe it clean.

All in all, the current digital landscape poses significant opportunities for modern digital workers to lean into where and how they want to do work – often accelerating business outcomes as a result. But without the right security tools or trainings in place to support the use of mobile devices and BYOD at scale, the mobile workforce could inadvertently create a security nightmare for enterprises.

As the digital landscape evolves, it's essential for CISOs and security teams to ensure they have visibility across infrastructure and networks to optimise, secure, and enable digital workers – across the devices of their choosing – without opening their organisations up to more risk. It's a tall order, but thanks to modern solutions and capabilities like MDM, it's more possible for modern enterprises to build and grow (securely) and at scale.

High-touch managed services - closing the cloud skills gap

Cloud technology now underpins how many businesses operate and grow. It enables organisations to innovate faster, scale with flexibility and access powerful tools without heavy infrastructure costs.

BY JON LUCAS, DIRECTOR AND CO-FOUNDER, HYVE MANAGED HOSTING

FOR MANY, the cloud is not just an IT choice but the foundation for resilience and future competitiveness.

Yet the scalability, collaboration, security and cost benefits are becoming harder to access, with 57% of UK businesses in Hyve's IT and Tech Skills Gap Report having an unmet need for in-house cloud computing skills, a reflection of the skills shortage in the wider industry.

The rapid pace of technological advancement, insufficient training and a shortfall in skilled applications from schools and universities have exacerbated the issue. In some cases, cloud projects are being slowed down or even shelved as businesses struggle to find knowledgeable and experienced cloud talent.

While improvements in the talent market are possible with targeted initiatives, businesses can't sit and wait for them to happen. If they don't take immediate action, the shortage of internal cloud expertise can create security gaps, leading to breaches or compliance failures that erode trust with customers and partners. In fact, the O'Reilly 2024 State of Security Survey report, finds that cloud security expertise remains a major concern, with 38.9% of respondents pointing to it as the most critical skills gap.

Yet, the problem extends beyond security. It can also result in costly outages or poorly executed migrations, which reflect badly on a company's reliability. Over time, these missteps signal to the market that the organisation lacks the capability to manage modern technologies, harming its reputation and competitiveness.

For SMEs, the impact is greater, as they compete with larger firms for scarce talent while working with tighter budgets and lean teams, and are therefore often forced to offer higher salaries. At the same time, limited budgets and lean teams mean even small missteps can drain resources, damage credibility and slow growth, leaving them less able to compete against larger, better-resourced rivals.

Finding a way forward

An alternative solution is needed to bridge the skills gap and provide an immediate impact for SMEs in particular. MSPs are the partners that bring deep experience and specialist knowledge to the table, designing and deploying optimised cloud hosting solutions that meet the specific needs of a business. And they are becoming increasingly popular. Flexera's 2025 State of the Cloud Report highlights that 84% of organisations globally struggle to manage cloud spend and 60% now use

MSPs in some capacity. Opting for an MSP approach ensures the business has a range of external experts to call upon for support, 24/7. And by avoiding onboarding delays or hiring overheads associated with internal hires, businesses can save on costs at the same time.

Equally, using an MSP often delivers enhanced value over the long term.

With expertise in cloud strategy, these organisations can remotely manage a company's IT ecosystem and give smaller businesses access to the latest technologies and best-in-class providers that would be otherwise unattainable for SMEs. This can include helping with the right infrastructure, migration, management and optimisation.

From the security perspective too, they can handle key tasks such as managing protection settings, or implementing threat detection and monitoring, allowing internal teams to concentrate on essential business operations.

Making the right choice

Providers vary in approach and depth of service, so selection matters. When making a choice, companies should prioritise a high-touch approach that goes far beyond the transactional model of hyperscalers or MSPs driven by private equity.

Instead, they should favour providers that focus on building multi-year relationships rather than concentrating primarily on consumption growth or financial targets like many hyperscalers

do. This means opting for a partner that leads structured discovery workshops, designs reference architectures aligned to business and compliance needs, provides transparent cost models and guarantees measurable service levels supported by expert availability round the clock.

With these foundations in place, a high-touch MSP can move quickly to deliver tailored hosting environments for mission-critical workloads, ensuring consistent uptime and alignment with business objectives.

The best providers put relationships first, offering flexible management tiers, direct engineer access, and dedicated account managers, demonstrating a commitment to long-term trust and exceptional service rather than short-term profit.

Building confidence in the cloud

The cloud offers enormous potential, but the skills gap continues to hold many businesses back from realising its full value. For SMEs especially, the risk of missteps can be costly, both financially and reputationally.

By working with the right MSP, organisations can access the expertise, security and reliability needed to safeguard operations and drive growth.

High-touch managed services help bridge the divide between ambition and capability, enabling businesses to focus on what they do best while knowing their cloud infrastructure is resilient, secure and built to support long-term success.

Yet, the problem extends beyond security. It can also result in costly outages or poorly executed migrations, which reflect badly on a company's reliability. Over time, these missteps signal to the market that the organisation lacks the capability to manage modern technologies

The value of a network community

Building meaningful relationships in business has never been more important.

BY SIMON WEST, GENERAL MANAGER, NETWORK GROUP

RUNNING AN MSP or IT company can be a lonely pursuit. Many owners feel unable to air issues or concerns with their own team as they're expected to always have the answers – a pressure that can take its toll. Without a trusted peer group to turn to, business leaders can become stuck on challenges, without any clear path forward.

That's why structured business relationships matter. They allow owners to take time away from the business – to step back, share openly, and grow alongside those who are able to sympathise and advise on those same challenges.

Managed Service Providers (MSPs) and IT providers that don't have that outlet could suffer, missing out on not just knowledge sharing, but the support and perspectives that can make a massive difference in navigating modern IT challenges. On the other hand, those that put the time and effort into building mutually beneficial partnerships will be well placed to gain an edge, simply by exchanging ideas and knowledge.

It is within this context that network community groups have become so important. These are trusted spaces through which business owners and department heads can share experiences and advice with likeminded businesses to help them collectively thrive.

Whether you're running a five-person MSP or leading a larger IT operation, the challenges are often strikingly similar – just experienced at different scales. That shared understanding is a platform for empathy, practical advice, and genuine relationships that can help businesses thrive. It aids innovation, yes – but it can also be a pillar to lean on in tough times.

Naturally, founders and business owners may find it tricky to justify dedicating the time and resources required to effectively engage and draw the most from peer groups. These may be seen as a luxury or a nice to have. Yet, for many businesses, they can be a pathway to unlocking several key competitive advantages in multiple ways.

Strength in numbers

The core mission of industry support groups is mutual success, bringing together a varied expertise and experiences to be shared in the form of insights, knowledge and learnings that benefit the collective. It is for this reason that having a high volume of companies involved in a network group is beneficial.

From a commercial point of view, there's real strength in numbers. At Network Group, our average

member revenues are a little over £2 million, yet we're able to ask SaaS vendors and hardware providers to treat the collective as a £200 million organisation, and secure favourable commercial terms for our members. Further, having a united community can truly influence the wider market, and even drive change at the policy level, or among industry bodies. Key decision makers are more likely to listen to unified, collective voices, underpinned by a trusted network representing tens of businesses.

However, it's just as much about the quality of companies involved as it is the quantity. Bringing the right members together – those that are keen to actively engage with others, tell their stories, and share not only their wins but also their struggles – is key. That requires vulnerability at times, yet that vulnerability can lead to genuine conversations which can be of the greatest value.

When members feel safe to be honest about what's working, what's not, and what they're unsure about, the quality of collaboration dramatically improves, with conversations centred around real support and practical solutions.

Consider innovation. For technology providers, where agility and adaptability are critical to staying competitive, a trusted peer group can dramatically shorten innovation cycles. Take artificial intelligence as an example: instead of experimenting in isolation, members can share early experiences with AI-driven automation or service delivery tools, exchange feedback, and refine their approaches together. The result is faster, lower-risk adoption of emerging technologies than traditional external channels typically allow.

Raising the bar for everyone

Inter-company support, business development sessions, benchmarking opportunities against industry peers – there is so much peer groups can offer beyond the direct commercial merits. They provide a space in which members can see their own challenges in others, and gain reassurance they're not alone.

When members feel safe to be honest about what's working, what's not, and what they're unsure about, the quality of collaboration dramatically improves, with conversations centred around real support and practical solutions

At a time in which the tech landscape continues to evolve at speed, having a steady, supportive network of industry peers and access to key learning resources can make a pivotal difference – a community that businesses can count on for practical support. From scaling operations to managing talent, companies are facing similar issues.

To be successful, community groups are the way to go. It can be natural for business leaders to feel protective – to want to be secretive about their best solutions and learnings to try and get ahead of the competition. But who is really going to be successful? A single isolated company, or tens of collaborative peers sharing their best innovations and insights collectively? The modern way of doing business is not about ring-fencing and restricting knowledge, but swapping ideas, being free and open with information, and generous with your knowledge and time.

MSPs need to embrace this cultural shift towards collaboration – to see the value in openly sharing strategies, mistakes, and insights. It's not about outdoing each other. It's about raising the bar for everyone and driving collective progress.

AI isn't as exciting as the Premiership, but it can kick-start your ESG strategy

With two managers gone, countless VAR dramas, and a physio room that's busier than a sales desk at the end of Q4, the Premiership moves fast. So does AI.

BY ROSS TEAGUE, CEO NEBULA GLOBAL SERVICES

IT'S NO SURPRISE that for many MSPs, Environmental, Social Governance (ESG) goals have slipped a few places down the priority table. When you're juggling growth, client demands,and cash flow, finding time for sustainability planning feels like chasing a ball that's always two yards ahead.

However, that doesn't have to be the case. Used carefully, AI can help the channel make real ESG progress, not through expensive, complex rollouts, but by giving teams clean data, freeing people from admin and dull reporting, and uncovering insights no one had time to follow up on before.

Start where your data already lives

Our ESG Unwrapped research showed that the best starting point is to use the data you already have. Basic AI-powered extraction tools can pull emissions-relevant data from invoices, travel claims, facilities logs, and supplier contracts. This will give a snapshot of where your Scope 1, 2 and 3 emissions actually lie without weeks of manual reconciliation.

Once you know where your biggest emissions and costs sit, you can prioritise what to do about them. It might be automating data collection for supplier reporting to save admin time or consolidating local courier jobs so they can be done more efficiently. It's not complex, just previously invisible.

Make the office your training ground

The same principle applies inside your own walls. Simple AI tools and devices can help you monitor out-of-hours energy use, sort recycling, and track water and waste use. Smart plug-and-play devices can track usage, identify unusual patterns and generate data that's easy to feed directly into your ESG reporting. Many partners are already using AI tools to help analyse waste and procurement, cutting over-buying on peripherals and packaging. Travel analysis can suggest lower impact routes or encourage salespeople or execs to meet online when is physical trip is unnecessary.

Scope 3 is the toughest opponent

Scope 3 data is still the toughest opponent. Suppliers send information in different formats, if they send it at all, so Scope 3 becomes a laborious task to get missing information. That's where small language models (SLMs) can help. Many SLMs are available free on platforms like Hugging Face and can run securely on local hardware, so your data never leaves the building.

Trained on supplier documents, contracts and policies, an SLM can read statements, pull out any references to emissions or recycling commitments, and summarise what's missing. It can even flag when a supplier's claims are vague or out of date.

This turns piles of unstructured information into a clear list of who has solid sustainability data and who still needs following up. Over time, it gives you a much clearer picture of your indirect (Scope 3) footprint, without adding too much to anyone's workload.

With AI, it's important not to go offside Good governance keeps things onside. That doesn't mean writing a 40-page policy; it means setting a few clear boundaries. Know which data is fair game for experimentation, keep people in the loop when AI is being used to inform reports, and log what's automated.

Most importantly, write it down in plain English. Transparency helps when auditors or clients ask how you got your numbers, but it also builds trust across your own teams. Don't forget to involve the people who own the process.

The best ideas can come from ops, finance, facilities (or even the sales and marketing teams!), it's not just IT.

We've also got to be honest about AI's own footprint. Training large models consumes energy and water, although much depends on where and how they're run. The right response isn't to avoid AI altogether (that ship has already sailed), but to find a better balance between the environmentalcosts and gains. Currently, the thinking is that, unless you're a hyperscaler or huge corporate, it's more likely your business will save more resources than AI consumes.

Play to the final whistle

The partners leading the way in our research weren't the ones with the biggest budgets. They were the ones willing to start small, experiment, and share what they learned.

Start with the data you have, have an ESG goal in mind, and use AI to help you reach that goal one step at a time. And unlike some VAR decisions, your results won't be overturned on review.

Good governance keeps things onside. That doesn't mean writing a 40-page policy; it means setting a few clear boundaries. Know which data is fair game for experimentation

MSP CHANNEL AWARDS 2025 WINNERS

advania · ARROW · CHECK POINT · intergence · Kaseya · LapSafe · infinigate cloud · opengear A DIGI COMPANY · opentext Cybersecurity · SOPHOS DEFEAT CYBERATTACKS · SOTS · StorMagic

SPONSORED BY: EXAGRID · cyberglobal

Put a price on security with value at risk

According to Gartner, companies will spend $118.5 billion on cyber security solutions worldwide and the market will expand by 14% during 2025. The growth of new technologies like generative AI and increased cloud deployments will grow companies' attack surfaces too.

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

WHILE the amount of money going into security might go up, the sheer scale of attacks and attempts on companies will stretch those budgets significantly.

At the same time, the number of companies competing to deliver those solutions is growing too. According to Compubase, there are 7,500 companies involved in delivering security solutions to customers in the UK alone, ranging from resellers and partners through to managed service providers and systems integrators. With so many companies involved, and so much noise around new threats to navigate, it should be no surprise that companies face challenges in differentiating themselves in the market.

To be successful in this complex and complicated market, you have to cut through to what customers really care about. Looking at Value at Risk can help.

What is VAR, and why should a VAR care?

The acronym VAR has long stood for Value Added Reseller, and many channel companies focus on how they can add services or consulting to their product sales. The concept of Value at Risk aims to help these companies go further with their customers around long-term security needs.

Value at Risk - hereafter VAR - involves helping customers to understand the real world monetary cost that security issues represent. This involves going into cyber risk quantification (CQR) where you help customers understand both the cost of a potential issue in terms of lost revenue and how likely that issue is to take place. By putting things directly in monetary terms, security teams can express the threats and risks that businesses face without resorting to technology jargon. It also makes it easier to categorise and prioritise those risks based on impact.

VAR might seem obvious - surely every company does this? - but the answer is that many companies don't have a full operational process that categorises risks over time. Celebrity IT security issues that get all the attention might attract the board's attention, and then get a full write-up, but those issues may not be relevant or risky to the company itself. This then becomes a distraction. Alternatively, threat intelligence might come in that changes that risk level from one day to another - how can you

get the board to understand that risk over time, and what your customer's team is already doing to prevent it?

Putting money against risk scores makes it easier to put things in business terms. It also makes it easier to justify prioritising certain issues rather than others. For example, take two security issues that affect two of the organisation's business lines - which one should you prioritise? Without context, it is hard to know. But say one issue has a ten percent chance of affecting the business, and the other has a twenty percent chance ... the one that is more likely to take place will take precedence over the other. But hang on. The issue rated at ten percent is in a business unit that makes £200million a year, while the twenty percent issue in one that makes only £20million a year. Now, the risk is £20million compared to £4million, changing priority again. Using VAR helps you - and your customers - make decisions over time around what to prioritise, what to mitigate and where you might need cyber insurance too.

Implementing a risk operations centre CRQ is an established approach to pricing risk. It's something that security leads in enterprises want to use, but many of them are not able to make this an operational process. According to Gartner, only a third (36 percent) of cyber security leaders have made CRQ effective enough to support actions while the analyst firm also estimated that around half of all CRQ projects would potentially fail by 2025. To avoid this, companies need to make risk management into an operational process, just like IT security did in the past.

This does require a different mindset compared to looking at the technology or products installed. Instead, it involves creating a specific flow for data from multiple vendors or providers that can then be synthesised effectively into one set of results around potential risk. By turning this into a risk operations process, rather than looking at the results on any one issue, security teams can provide better insight.

For channel companies, this independent approach is a natural starting point. Rather than relying on any one vendor, channel partners are already keen to provide that insight to their customers around risk data.

Helping customers to implement a Risk Operations Centre (ROC) to complement their Security Operations Centre (SOC) provides that framework for risk management. Alternatively, partners can provide managed ROC services to their customers, where that data is delivered as a service based on customers' deployments and potential security gaps.

To achieve this, you can deliver risk advice that looks at the specific assets that your customers have, what issues exist in that environment, and the threat intelligence that is being released over time. As new threats are discovered, or new attack chains are developed, these risks can be scored and then used to inform the business. More importantly, the risk data can be translated into the potential costs and cash impact - otherwise known as VAR - that those threats can have.

Using money values in this way makes it easier to explain to customers around risk impact, and demonstrate the specific ways that risk can be reduced, mitigated or eliminated. The most important element here is that this is more than any one product - it is about the whole approach to managing risk based on what is valuable.

Long-term risk

As the security sector continues to evolve and respond to changes in the wider IT industry, IT Security teams will have to secure more infrastructure elements and deliver results across more assets, software and data. That growth of IT around elements like AI will stretch budgets further. In response, teams have to look at the specific risks that are coming up and prioritise which ones really matter.

Understanding those risks involves looking at the money aspect, and the level of risk is based on the cost that they could lead to. For the channel, helping customers to define Value at Risk helps them define and improve their approach to security.

MANAGED SERVICES SUMMIT

BENELUX
LONDON
NORDICS
MANCHESTER

CREATING VALUE with MANAGED SERVICES

managedservicessummit.com

MANAGED SERVICES SUMMIT BENELUX

benelux.managedservicessummit.com

30 JUNE 2026

MANAGED SERVICES SUMMIT LONDON

london.managedservicessummit.com

09 SEPTEMBER 2026

MANAGED SERVICES SUMMIT NORDICS

nordics.managedservicessummit.com

05 NOVEMBER 2026

MANAGED SERVICES SUMMIT MANCHESTER

manchester.managedservices summit.com

17 NOVEMBER 2026