BIRMINGHAM MSP
ROADSHOW

VIEWPOINT

BY SOPHIE MILBURN
EDITOR

AI in the channel: why MSPs must move intelligently, not recklessly

At our recent MSP Channel Insights Roadshow in Birmingham, one comment particularly resonated with me. One attendee stated that cybercriminals can afford to take risks with AI. They can make mistakes. They can compromise their own data. MSPs can't. It's a sobering truth. 'Bad actors' iterate without governance, compliance frameworks or reputational risk. They experiment in the dark, fail fast and pivot. Managed service providers, by contrast, operate in the full glare of accountability. One misstep with AI-driven automation, one hallucinated report, one compliance breach, and trust erodes instantly. That imbalance helps explain why attackers often appear ahead.

Despite this, the mood across the channel is one of cautious optimism. There's clear recognition that AI will play a meaningful role in service delivery, but adoption is measured. Governance, data protection and client trust sit at the core, meaning experimentation is deliberate and tightly controlled. The hesitancy isn't about doubting the opportunity; it's about understanding the responsibility. Still, the question many are beginning to ask is whether being cautious now carries its own risk.

The 'AI is a bubble' refrain surfaced, less as dismissal, more as caution against the hype cycles that inflate expectations beyond reality. So, can MSPs afford to be cautious anymore? In 2026, the answer is complex. The challenge now is twofold: adopting AI in a way that is secure and governed, while also moving fast enough to keep pace with change. That means shifting the core question from "Should we use AI?" to "Where can we deploy it safely, measurably and transparently, and how quickly can we scale what works?" It's about striking the balance between careful governance and the speed required to keep pace with rapidly evolving threats.

What struck me most is how AI is no longer confined to its own category. It now underpins conversations across marketing and innovation, compliance, workforce transformation and cyber resilience, as a strategic layer across the entire business. The goal isn't to produce more content or more noise. It's to use AI to drive real efficiency while preserving the judgement, creativity and empathy that will set an MSP apart. That's especially true in marketing, where human psychology, nuance and authenticity matter. The advantage won't come from using AI everywhere, but from using it thoughtfully to enhance human insight, rather than dilute it.

Bad actors may move recklessly. MSPs must move intelligently. In 2026, success won't come from chasing the latest AI feature, but from building resilience and embracing evolution at pace. The channel has always adapted; now it simply has to do it faster.

Contents

Cover Story

Birmingham MSP Roadshow sparks insight, debate and collaboration

MSP leaders came together at Hotel Du Vin for a day of meaningful discussion, candid peer conversations, and practical strategies, exploring the challenges and opportunities shaping the channel today.

12

18

`32`

NEWS

`06`

`11`

Wipro launches AI-enabled operating model for enterprise functions

Wipro presents an AI-enabled approach to enterprise processes, combining consulting and automation for improved operational delivery.

WIPRO LIMITED has announced a new operating model aimed at enhancing enterprise functions. By merging advisory, artificial intelligence, and comprehensive enterprise transformation services, the initiative aims to enhance core business areas including People & Change, Supply Chain & Operations, Finance Transformation, and Sales, Marketing & Customer Experience (CX).

The model seeks to link strategic boardroom decisions with scalable operational processes. The model is intended to turn innovation into an ongoing process, supporting Wipro's role in modernising and optimising core enterprise functions.

Wipro's new integrated model relies on consultancy as the initial transformation catalyst, redefining conventional service models. The solution employs the Wipro Intelligence suite, which offers AI-driven solutions across the client engagement lifecycle. This aims to ensure AI's systematic application, aligning with concrete business outcomes.

At the onset, Wipro Consulting will guide clients through their journeys, collaborating with key executives to define AI strategies, envision future operational models, and lay out outcomes.

During the solution design phase, the consultancy teams will craft AI-enhanced, people-centred operational models. This includes re-engineering processes and scenario modelling to transition from design to execution.

Utilising the Wipro Intelligence suite, Business Process Services (BPS) teams will execute AI-facilitated automation, deliver predictive insights, and ensure continuous improvement across business operations. These AI-centric models, designed for ongoing improvement, seek to facilitate

> During the solution design phase, the consultancy teams will craft AI-enhanced, people-centred operational models. This includes re-engineering processes and scenario modelling to transition from design to execution

quick bottom-line impact, improved economics, and sustained results.

"Reimagining business processes in the age of AI is core to our clients' enterprise business transformation strategy," said Jasjit Singh Kang, Managing Partner and Global Head of Business Process Services, Wipro Limited. "AI-embedded operations, underpinned by deeply contextual solutions, are the future of the intelligence-driven enterprise. This new integrated model will help us deliver on our clients' demands to build AI solutions designed around persona-based and function-specific processes so they can drive measurable outcomes and real bottom-line impact."

As the industry evolves, Wipro's strategy aims to embody the shift towards persona-specific, AI-embedded operations. This model aligns with efforts to modernise intelligence-driven enterprise processes, supporting measurable outcomes and improvements for clients.
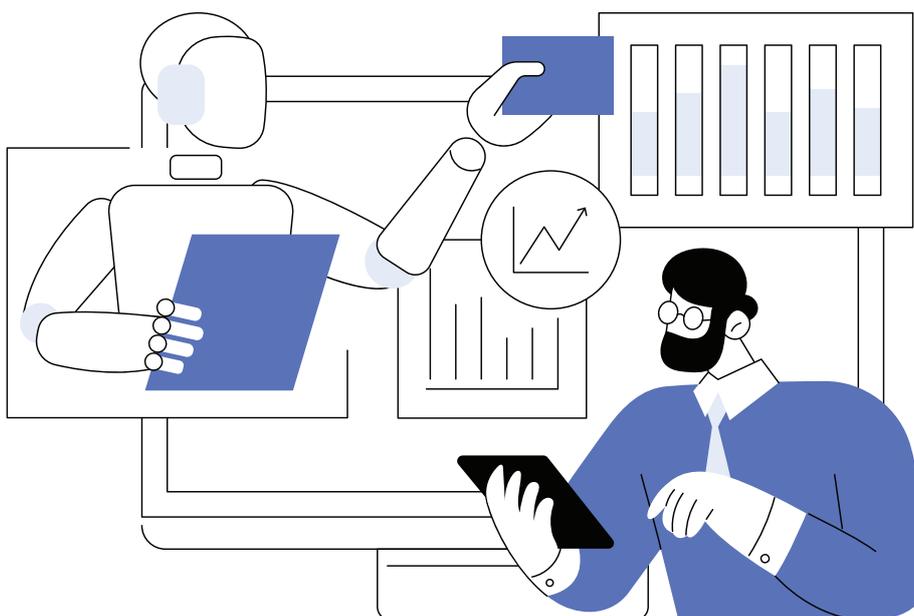
Government and defence agencies face growing cybersecurity risks

New reports indicate growing cyber threats for government sectors, underlining the urgency for integrated cybersecurity measures.

NEW RESEARCH FROM EVERFOX, a cybersecurity company, has revealed concerns among government IT security leaders. Their report finds that 84% of these professionals agree that sharing sensitive data across networks exacerbates cyber risks. More than half still rely on manual data transfer processes, even as artificial intelligence accelerates operational tempos.

The recently published CYBER360: Defending the Digital Battlespace report, based on surveys of 500 security leaders and IT decision-makers in the U.S. and UK, paints a picture of escalating threats. National security organisations reported facing an average of 137 cyberattacks weekly in 2025, compared to 127 in 2024.

Notably, the U.S. agencies were found to experience a 25% rise in attacks compared to their UK counterparts.

With digital transformation reshaping the 'battlespace', trusted data's secure movement is considered essential for mission success. However, survey participants highlighted several challenges:

- 78% identified outdated infrastructure as a significant vulnerability, pointing to analogue systems and manual processes undermining secure data exchanges.
- Nearly half, 49%, consider maintaining data integrity during cross-network transfers as their primary hurdle.
- A significant 45% grapple with

managing identity and authentication across various domains.

The CYBER360 report highlights an urgent need to evolve beyond traditional network defences. Adopting a new model combining multiple protection layers could be a solution. By employing three cybersecurity frameworks - Zero Trust, Data Centric Security (DCS), and Cross Domain Solutions (CDS) - agencies can aim to ensure secure, real-time data exchange across mission-critical systems.

This integrated approach seeks to enhance operational resilience and mission assurance, making it important to the future of digital security in government sectors.

NinjaOne enhances IT monitoring with integrated asset management solution

NINJAONE has introduced NinjaOne IT Asset Management (ITAM), a feature designed to provide visibility and control over IT environments by integrating endpoint and asset management within a single platform.

The addition of ITAM allows organisations to extend asset lifecycles, manage costs, strengthen security, and support compliance. By consolidating asset data into actionable insights, organisations can improve IT infrastructure management.

As IT environments grow more complex, organisations face challenges in tracking and managing hardware, software, and connected systems. According to IDC, over 90% of organisations manage both installed

software and SaaS, while more than 80% also manage cloud assets and mobile devices. Accurate asset data is increasingly important to support functions across procurement, finance, and IT operations.

NinjaOne ITAM combines asset management with endpoint management, providing a unified inventory that continuously syncs asset data in real time. This supports faster, informed decision-making and simplifies day-to-day IT operations. For large-scale IT environments, ITAM integrates with IT Service Management (ITSM) workflows to help streamline decision-making across IT functions.

Key benefits include:
- Reduced costs and longer asset

lifecycles: Real-time hardware and software tracking, along with automated warranty management.
- Enhanced security: Ability to identify unmanaged devices and understand their connections to reduce risks.
- Streamlined compliance: Real-time records of devices and dependencies support audits and regulatory standards.
- Operational intelligence: Integration with ITSM workflows enables proactive management of assets, changes, and incidents.

Christian Lewin, Head of IT Operations at Popken Fashion Services, said: "With NinjaOne, we now have a unified view of all assets, from rollout to subsequent service, complete with an audit trail for all systems."

Joseph Vito joins Rackspace as Senior VP of Partnerships

Rackspace Technology adds Joseph Vito to lead global alliance partnerships.

RACKSPACE TECHNOLOGY, a hybrid cloud and AI solutions provider, has announced the appointment of Joseph Vito as Senior Vice President of Strategic Alliance Partnerships. Vito will play a role in leading Rackspace's global strategy, focusing on cultivating and enhancing technology and channel partnerships that drive innovation while providing value to customers.

Joseph Vito joins Rackspace with over 25 years of experience in technology leadership, cloud transformation, and enterprise solutions. His extensive career spans across various sectors, including financial services, life sciences, energy, and consumer manufacturing. His most recent role was as a Strategic Transformation Principal

at Amazon Web Services (AWS), where he aided organisations in developing cloud adoption strategies and migrating from legacy systems to advanced cloud-based solutions.

Prior to his time at AWS, Vito held the position of Transformation Advisor at Dell-EMC, where he assisted clients with the design, investment, and deployment of integrated solutions, notably encompassing DevOps and workload management. His career also includes leadership positions such as CIO for UBS AG's Global Data Services division, CTO and Head of Data Operations at Dun & Bradstreet, and CTO/CIO roles at US Trust & Merrill Lynch, focusing on steering technology strategies and integration initiatives.

Joseph Vito holds a Bachelor of Arts in Managerial Economics from Union College and a Master's Degree in Finance from Pace University, helping demonstrate his academic background to complement his industry expertise.

Snowflake and OpenAI partner to enable AI insights for enterprises

SNOWFLAKE, a provider in the AI Data Cloud sector, has announced a $200 million partnership with OpenAI to develop and deploy AI solutions for global enterprises.

Central to this alliance is the integration of OpenAI's models directly within Snowflake's platform, Cortex AI. This feature aims to empower key clients, including Canva and WHOOP, to leverage these models for intricate data insights. OpenAI models, such as the GPT-5.2, are now readily accessible, enabling organisations to exploit their enterprise data.

Snowflake's CEO, Sridhar Ramaswamy, highlighted that their platform permits organisations to construct and utilise AI on their most valuable asset — data. This secure governance ensures businesses can build AI agents that embody strength and responsibility. Concurrently, OpenAI's CEO of

Applications, Fidji Simo, noted that this collaboration facilitates the closer deployment of AI agents alongside business applications, bridging the prevalent AI capability-value gap.

Helen Crossley from Canva expressed excitement about employing OpenAI models through Snowflake Cortex AI, aiming to enhance their platform's scalability and AI offerings.

Similarly, Matt Luizzi from WHOOP acknowledged the impact of Snowflake Intelligence in decision-making, stating that having OpenAI's capabilities within Snowflake would refine their analytical processes without compromising security.

Intended benefits identified from this partnership include accelerated product innovation using OpenAI's Apps SDK, AgentKit, as well as developing

adaptive AI agents that harness governed data to deliver impactful intelligence.

Snowflake and OpenAI are collaborating to enable businesses to use AI for accessing data. Their approach allows employees to query both structured and unstructured data using natural language.

Finally, Snowflake aims to ensure governance and reliability, with a 99.99% uptime SLA. This aims to ensure that enterprises can reliably infuse OpenAI's models into their workflows, safeguarded by the governance standards of Snowflake Horizon Catalog.

The collaboration builds on the existing relationship between the two companies, supporting joint efforts in AI development and workforce productivity initiatives.

TeamViewer and Thrive join forces to enhance digital workplaces

TeamViewer partners with Thrive to integrate DEX capabilities into its managed services platform, improving operational visibility and workflow efficiency.

TEAMVIEWER has announced a partnership with US-based managed service provider Thrive. The collaboration integrates TeamViewer's Digital Employee Experience (DEX) capabilities into Thrive's NextGen managed services platform, adding insight and automation to its ServiceNow environment.

Thrive's platform is designed to provide clients with operational visibility while reducing complexity across modern IT environments. Built on ServiceNow, it combines automation, AI, security operations, and network operations into a consolidated, scalable framework. With TeamViewer DEX, Thrive can identify potential issues earlier and

address them before they affect users, helping to reduce support demand and maintain service quality.

Managed service providers face the challenge of moving from reactive support models toward continuous optimisation. With additional visibility into endpoint performance and employee experience, Thrive can incorporate enhanced automation and remediation into its ServiceNow workflows, supporting clients in running more stable and efficient IT environments.

Oliver Steil, CEO of TeamViewer, noted that the partnership supports a more proactive approach to IT operations,

allowing issues to be addressed with greater precision. Bill McLaughlin, CEO of Thrive, said that client experience remains central to the company's operations. Scott Steele, COO of Thrive, highlighted that the integration leverages AI, automation, and DEX capabilities to strengthen Thrive's platform and IT service delivery.

The partnership reflects a shared goal of evolving managed services beyond traditional monitoring and ticket-based support. By embedding DEX into Thrive's platform, IT organisations gain insight and automation tools to improve digital workplace outcomes, positioning IT as a contributor to business operations rather than solely a cost centre.

Kyndryl introduces SAP Centre of Excellence for modernisation and AI adoption

KYNDRYL, a provider of enterprise technology services, has announced the launch of the SAP Transformations Centre of Excellence (CoE). The CoE is a dedicated hub where customers can work with Kyndryl's designers and engineers to explore the application of AI in SAP transformations.

Within the CoE, customers can collaborate with experts to design, develop, and deliver SAP solutions at scale.

Key elements of the initiative include:
- Clean Field approach: Using Nova Intelligence AI agents and Kyndryl's Data Transformation Suite to accelerate transformations from SAP ECC to SAP S/4HANA. This method aims to reduce technical debt and support quicker, more cost-effective

SAP modernisations while enabling scalable business capabilities.
- Clean Core: In collaboration with Nova Intelligence, Kyndryl provides an AI- and data-driven approach for customers on SAP S/4HANA, supporting the modernisation of custom code while adopting new capabilities.
- SAP Business Data Cloud: Leveraging SAP BDC to unify enterprise data and integrate with Databricks for AI training. This provides a foundation for scalable and responsible AI implementation with measurable business impact.
- Journey to RISE with SAP: An expanded partnership delivering SAP S/4HANA Cloud Private Edition services, assisting organisations in accelerating cloud migrations and modernising SAP environments to support AI at scale.

Kyndryl has applied these approaches in practice. For example, the company supported an Austrian industrial food company in transitioning from SAP ECC to SAP S/4HANA using the Clean Field approach. In collaboration with Nova Intelligence, Kyndryl deployed AI agents to accelerate the move to SAP S/4HANA and achieve full Clean Core compliance. This reduced project duration and labour while establishing a platform designed for future adaptability.

Using the Agentic AI Framework, Kyndryl integrates AI solutions into customers' SAP platforms, enabling adoption at scale and supporting business outcomes.

The SAP CoE builds on Kyndryl's long-standing partnership with SAP and its status as a global delivery partner for the RISE with SAP programme.

Veeam software updates senior leadership with three key appointments

Veeam Software strengthens its executive team with three new strategic appointments to drive innovation and enhance global partnerships.

VEEAM SOFTWARE has announced three senior leadership appointments as part of its ongoing organisational development. The changes include Brandt Urban as Chief Business Development Officer (CBDO), Tony Colon as Chief Customer Officer (CCO), and Michael Rau as Vice President of Worldwide Partners.

Anand Eswaran, CEO of Veeam, noted that the company continues to focus on data resilience, security, and AI, and that these appointments aim to support growth and strengthen partnerships.

Brandt Urban: Chief Business Development Officer

Brandt Urban has been promoted to CBDO, where he will oversee corporate development, mergers and acquisitions, strategic partnerships, and corporate strategy. Previously, he led cloud sales at Veeam and will now focus on ventures, alliances, and acquisitions to support the company's offerings in data resilience and AI.

Tony Colon: Chief Customer Officer

Tony Colon takes on the newly established CCO role, responsible for managing the full customer journey, including satisfaction, retention, and service delivery. He brings prior experience at companies including ServiceNow and Cisco and will support Veeam's initiatives in data resilience and cybersecurity.

Michael Rau: Vice President of Worldwide Partners

Michael Rau joins Veeam to lead the global partner business, developing programmes and solutions with partners including HPE and Lenovo. His role aims to enhance Veeam's engagement with its partner ecosystem.

John Jester, Chief Revenue Officer at Veeam, highlighted that these appointments support the company's objectives for customer and partner engagement, as well as continued development in data resilience and related technologies.

Guardz reports AI-driven growth and strategic partnerships in 2025

IN 2025, GUARDZ reported substantial developments in its cybersecurity offerings for Managed Service Providers (MSPs) and IT professionals, providing unified cyber protection for small businesses. The company recorded 300% year-over-year growth in annual recurring revenue, reflecting increased demand for its AI-native detection and response platform.

With a workforce exceeding 100 employees, Guardz's operations and global expansion were supported by a $56 million USD investment secured earlier in the year, providing resources to further develop its platform and services for the MSP community.

During the year, Guardz expanded its strategic partnerships, including agreements with Check Point and SentinelOne, which enhanced

the platform's capacity to address ransomware, business email compromise, and other advanced threats. A partnership with Pax8 extended the company's reach among MSPs.

Product updates in 2025 included the introduction of the wUltimate Plan, designed to streamline security operations for MSPs, and the launch of Identity Threat Detection and Response capabilities to address identity-based attacks. The Guardz Research Unit (GRU) was also established, providing monitoring of dark web activity, unpatched vulnerabilities, and ransomware-as-a-service threats.

Guardz's solutions are now used by thousands of MSPs to protect tens of thousands of small businesses worldwide. The company received

several industry recognitions, including the Global Infosec Awards, MSP Today Product of the Year Award, and Top InfoSec Innovator Award, as well as finalist placements in the SC Awards Europe and CRN Tech Innovator Awards.

Looking forward, Guardz plans to continue developing its cybersecurity platform, expand its global presence, and participate in upcoming industry events such as the MSP Expo and Right of Boom conferences.

> Guardz's solutions are now used by thousands of MSPs to protect tens of thousands of small businesses worldwide

Securing AI integration: Teleport's agentic identity framework

Explore Teleport's new framework for integrating AI agents securely into enterprise infrastructure without compromising data integrity.

TELEPORT has unveiled the Teleport Agentic Identity Framework, an AI-focused framework designed to support organisations in deploying agentic AI across cloud and on-premises environments.

The framework emphasises security and identity, providing a structured approach to operating autonomous AI while reducing risks of data misuse and external threats.

The framework addresses a challenge faced by many enterprises: the rapid deployment of AI agents, which can complicate the secure management of these dynamic, non-deterministic systems.

Designed to close this security gap, the Agentic Identity Framework provides a roadmap for organisations to integrate AI while maintaining security and compliance.

Identity management and agentic AI

Agentic AI introduces new operational challenges, as systems act with autonomy, dynamically accessing data and executing tasks. Traditional security and identity frameworks are not designed to manage these types of operations at scale.

A survey conducted by Teleport of more than 200 infrastructure leaders found that 69% expect significant changes to identity management due to AI. These results indicate that conventional identity solutions may be insufficient for large-scale AI deployments.

Current approaches, relying on static credentials or fragmented identity management systems, can create systemic risks, particularly as AI deployments expand.

Teleport's unified identity platform

The framework introduces a unified identity layer, secured through cryptographic methods and a hardware root of trust. This layer supports zero-trust authentication and provides real-time visibility into identity operations. By replacing static credentials with ephemeral identities, it aims to prevent unauthorised access and mitigate identity-related threats.

Framework relevance

Many solutions focus narrowly on AI safety or runtime monitoring, without addressing trust at the identity level. The Teleport Agentic Identity Framework positions identity as a central security control for agentic AI in enterprise environments.

Frank Dickson of IDC noted that identity, rather than monitoring alone, is a key control for securing AI systems, particularly at scale.

The framework:
- Treats AI agents as identities with cryptographic protection and auditing.
- Supports open standards to reduce vendor dependency and enable future scalability.
- Provides consistent identity governance across AI agents, tools, and infrastructure.

As AI deployments increase, unified identity management becomes essential. The framework addresses identity fragmentation, enhancing operational reliability and security, and establishing identity as the foundation for trusted AI integration.

Birmingham MSP Roadshow sparks insight, debate and collaboration

MSP leaders came together at Hotel Du Vin for a day of meaningful discussion, candid peer conversations, and practical strategies, exploring the challenges and opportunities shaping the channel today.

Fireside chat: Lessons in growth, automation and talent

THE DAY OPENED with a fireside chat featuring a high-growth MSP discussing lessons in scaling, resilience, and innovation. Nicola Saner of Chorus Cyber spoke about the benefits of becoming MXDR verified, highlighting recognition and verification as key advantages alongside growing profit margins through automation. She addressed pressing challenges when acquiring businesses, particularly around remote working, culture, relationships, and training and development, noting that these are easier to manage with a strong organisational culture and management that demonstrates integrity.

Nicola discussed the focus on SMB/SMC markets and the Microsoft stack,

emphasising a Microsoft-only approach. Looking ahead, she spoke about AI, stating, "I just want to get that pin and put it in the bubble and pop and then let's move on with AI properly." Saner also focused on culture, retaining staff, and equality in the workplace, highlighting how a curiosity-first mindset can motivate and retain the people crucial to their workforce. She also emphasised hiring for diversity, noting that the different perspectives it brings are what drive innovation. She concluded by reinforcing that "it's about getting the right people in the right places with a really curious mindset."

Building resilient defences in an AI-driven threat landscape

The event featured four panel sessions exploring the core pillars of MSP

success. The first panel 'Cybersecurity & Resilience – Navigating Threats in an AI-Enhanced World', saw Blake Neville (OneAdvanced), Gavin Roberts (Topsec Cloud Solutions) and Stephen Richardson (Digital Origin Solutions Limited) examining how MSPs can adapt to more sophisticated threat actors and build more resilient security strategies. The discussion explored what cyber resilience looks like in practice, noting that it is often treated as a buzzword but requires continuous testing and integration.

Blake Neville stressed that resilience is measured through ongoing validation, stating, "You're only as good as your last review or your last test of your business continuity or disaster recovery plan" and adding, "It's completely pointless having a business continuity plan unless it is embedded in your organisation." Gavin Roberts reinforced the importance of consistent testing and monitoring, saying, "It's not just a case of you plug something in and the security is done." Stephen Richardson emphasised the key questions organisations should be asking, including, "How is my data kept? Where is it kept? How quickly can I get back up and running?", to highlight operational readiness rather than reactive responses. The discussion also covered maintaining an evolving technology roadmap, addressing ransomware threats to small businesses, and layering threat intelligence as part of resilience strategy.

Winning through differentiation and smarter go-to-market strategy

The second panel, 'Smarter Sales &

Marketing – Winning in a Crowded MSP Landscape', moderated by Geoff Undrell (Asgard Marketing Limited) and featuring James Yates (Ingram Micro), Niall Mackey (Topsec Cloud Solutions) and Rob Jones (Jones Technology), explored how MSPs are evolving their go-to-market strategies through data-driven decision-making, AI adoption and vertical specialisation to drive profitable growth. Geoff stated, "knowing how you are going to differentiate yourself and position yourselves in the market is really important."

James Yates highlighted patterns of success driven by deep customer understanding, strong vertical focus and defining an ideal customer profile, while Niall Mackey emphasised knowing clients well and having the confidence to guide them on their needs. Rob Jones added, "The value is not the important bit, it's the business outcomes and making sure what we are doing is the right thing for the customer," reinforcing outcome-led selling. The discussion also stressed going back to basics - meeting clients, listening to them and engaging directly to build trust, loyalty and stronger relationships.

Talent, inclusion and authentic leadership

The third panel, 'People, Culture, Recruitment & DEI – The New Competitive Edge for MSPs', brought together Ian Luckett (The MSP Growth

Hub), Nicola Saner (Chorus Cyber) and Zoe Chatley (The Channel Recruiter). Nicola Saner expanded on themes from her fireside chat, reinforcing how strong talent strategy and inclusive culture are becoming key differentiators as MSPs scale. The discussion focused on attracting and retaining talent, particularly for challenging roles such as sales and consultancy. Zoe Chatley highlighted evolving candidate expectations and the importance of promotion from within, noting that younger talent in particular value progression opportunities, stating, "It's not just about money and benefits, it's about career development." She emphasised culture as a driver of staff retention and the need for flexibility, adding, "the more flexible you are, the more productive that individual will be."

Ian Luckett addressed diversity within the channel and questioned whether enough progress is being made, suggesting organisations need greater openness and vulnerability from leadership to challenge existing stigmas. He pointed to honesty, transparency and setting measurable targets around company values as ways to broaden access to talent. Nicola Saner concluded by stressing authenticity in diversity efforts, saying, "We have got to have diversity if we want to grow as businesses, but if you want to have diversity you have got to do it authentically."

Growth, valuation and the realities of M&A

The fourth and final panel, 'M&A, Investment & Growth Strategy – Building a Business That Scales or Sells', brought together Graham Stead (Growth Habits), Ken Roulston (Ex2 Consultancy), Malek Rahimi (BDR Group) and Rick Vogt (inTEC GROUP) to examine growth, valuation and acquisition trends in a fragmented UK market of around 12,000 MSPs. The discussion reflected differing views on the current ease of winning new business, alongside debate around valuations, preparation and what buyers are actually paying for as conditions begin to favour sellers again.

Rick Vogt highlighted rising M&A activity and noted, "If you've got the

Ian Luckett addressed diversity within the channel and questioned whether enough progress is being made, suggesting organisations need greater openness and vulnerability from leadership to challenge existing stigmas

right strategy around buying, you're obviously focused on opportunity." Malek Rahimi shared insights from scaling BDR Group from £9 million to £60 million, emphasising informed decision-making and adaptability, adding, "Tech is a fast-paced space. You blink fast and you'll miss it." Graham Stead outlined what buyers seek commercially, including strong customer bases and demonstrable growth potential, while Ken Roulston warned of disruption, describing AI as being both an opportunity and a threat, stating, "It has the capacity to fundamentally weaken and damage an MSP that doesn't recognise the threat of it and take sufficient action."

Peer-led collaboration and practical takeaways

Delegates participated in roundtable sessions hosted by Opentext, TopSec, and Growth Habits, rotating through focused discussions on pressing MSP challenges in a supportive and open environment. These breakout rooms encouraged candid conversations ranging from onboarding and API-first integration strategies to managing complex multi-vendor environments, while also exploring emerging threats, AI-driven security, and email protection. In the sales-focused session, participants explored the shift from founder-led selling to scalable, high-performance teams, covering pre-sales foundations, structured onboarding, aligned commission models and recruitment strategy. Attendees shared strategies for keeping teams motivated, building repeatable processes, and driving sustainable, long-term growth.

The roadshow wrapped up with a drinks reception, giving delegates the chance to follow up on ideas from the panels and breakout sessions

and discuss challenges facing their own businesses. Attendees left with clear takeaways on improving sales processes, strengthening cybersecurity, implementing inclusive recruitment strategies, and managing multi-vendor operations. By combining practical advice with open peer discussion, the Birmingham Roadshow reinforced the value of collaboration and knowledge-sharing in helping MSPs tackle real-world challenges and scale successfully.

We look forward to continuing these conversations at our upcoming MSP Roadshows in London (2 June), Dublin (23 June), Munich (6 October), Utrecht (12 November), and Copenhagen (24 November).

Further details on upcoming MSP Roadshow events can be found at https://msp-roadshow.com

Fast-growing MSP:
Why Infinity Group is one to watch

This feature is based on an exclusive conversation with **Infinity Group CEO Rob Young,** exploring the strategy and decisions driving the company's recent growth. Young reflects on the leadership principles and operational shifts that have shaped Infinity's growth, as well as the challenges and priorities that will define its next phase.

Introducing Infinity Group

HEADQUARTERED IN Tunbridge Wells, Kent, Infinity Group has become one of the UK channel's standout growth stories by taking a focused approach in a market where many MSPs expand their portfolios to chase scale. The company earned a place in the Fast-Growth 50 after its average monthly headcount rose from 58 to 99 between fiscal 2020 and 2023 (a 71% increase).

Infinity has strengthened its position as a pure-play Microsoft partner by replatforming around Dynamics 365, Business Central, Power Platform, Azure and Microsoft 365 to create a unified foundation for growth. That platform-led strategy has driven revenue growth of more than 60% since 2024 and supported targeted acquisitions that expand its ERP and vertical capability. With fixed prices, repeatable delivery models and an outcomes-driven approach that spans ERP, AI, data and cloud, the business is scaling with purpose while deepening its presence within the Microsoft ecosystem.

Culture and talent

Young explained that "culture is something you build into how the business runs." Rather than treating transformation as a separate initiative, it must be actively brought into the journey. He states that the company does not simply talk about AI, automation or platform strategy, it 'lives it'. By treating the business as the initial testing ground for the technology it implements, the company aims to ensure employees experience the same tools and transformation as customers. The vision is to create credibility and capability at the same time. Internal adoption strengthens practical understanding and supports ongoing development as technology and skills requirements continue to change.

Beyond technology adoption, culture is reinforced through inclusion and belonging. Infinity Group aims to provide employee resource groups, mentoring and community initiatives, and is intentional about creating space for different voices. Young adds: "When people feel invested in, challenged and equipped for the future, retention tends to look after itself."

Evolution of services

In its early days, like many managed service providers, Infinity Group operated in a more transactional way, delivering point-based services in specific areas. As the business matured, it became clear that customers were not struggling with individual tools, but with "disconnected systems and fragmented data." That insight has driven a clear shift in direction. Rather than focusing on standalone solutions, the company has shifted its model toward outcome-led transformation.

The emphasis is now on helping organisations build a single, scalable foundation that brings systems and data together. Frameworks such as its PIONEER approach to project delivery were developed to provide a structured and repeatable way for customers to realise value across multiple workloads.

More recently, AI has accelerated that evolution. As described by Young, it is no longer treated as a separate service line but embedded into how, CRM, service delivery and customer engagement operate together. The progression of services has been shaped by practical experience and by responding to what delivers measurable impact in the real world.

Practical adoption of AI

Young states: "AI isn't the strategy; it's an enabler," emphasising that the focus begins with data and process before introducing automation or intelligent agents. He adds that the priority has been to consolidate operations onto a more unified platform and streamline how the business runs. Only once those foundations were in place did AI become meaningful to apply at scale.

The team has focused on practical use cases for AI. That includes automating billing, improving finance workflows, strengthening sales qualification and reducing manual effort in service delivery. Simplicity and clear return on investment remain central to the approach.

He also highlights the tangible impact of this mindset, pointing to time savings, improved consistency and the ability to scale without proportionally increasing headcount. Beyond efficiency, the company sees AI as improving experience: customers receive faster responses and clearer insights, while
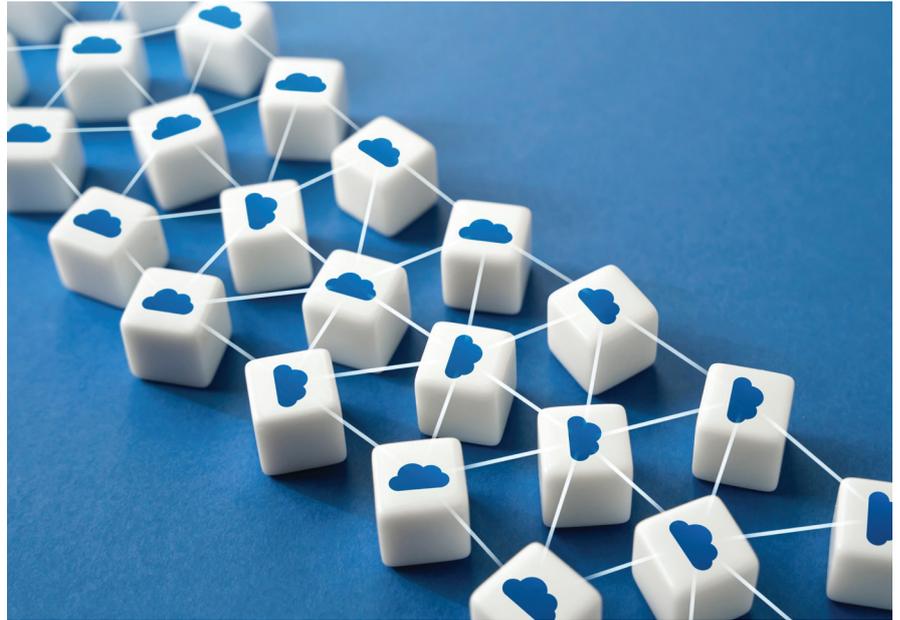
internal teams spend less time on repetitive tasks and more time solving higher-value problems.

Customer success and long-term retention

Young states that customer success is defined by outcomes over time rather than project completion. He says the focus does not stop at go-live, explaining that success is about whether customers are truly adopting what has been implemented and seeing tangible value from it. The objective is to deliver "better visibility, better control and better decision-making" for customers.

"A single integrated foundation allows deeper conversations about value. The focus moves beyond technical go-live to whether data is connected, processes are improving and automation or AI is delivering real operational impact. Young notes that when customers can see that progress clearly, "retention becomes a byproduct rather than a target."

Delivery models are built around shared ownership from the outset. Expectations are set early, success criteria are agreed and roadmaps extend beyond individual phases into ongoing optimisation. In his view, the goal is not to deliver one-off implementations, but to build long-term relationships where the business continues to support customers as their priorities evolve.

Leadership principles

As the business has scaled, Young says three principles have consistently

guided decision-making: simplicity, clarity and value. He explains that growth naturally brings more tools, more processes and more exceptions. If not managed carefully, that complexity can slow teams down and make it harder to adapt as the market changes. Decisions are therefore tested against clear questions about impact. He asks: "Does this add clear value? Does it reduce risk? Does it genuinely enable us or our customers to do something new or better?"

The discipline to maintain focus is central to his approach. "Saying no is often harder than saying yes, but it's essential if you want to build a business that can scale sustainably." That mindset reflects a broader philosophy during periods of rapid growth. The ability to decline opportunities that sit outside a clear vision can be just as powerful as pursuing new ones. A strong strategy combined with the confidence to say no can protect focus, culture and operational consistency.

Growth, challenges and advice

For Young, the biggest challenge during growth has been resisting short term fixes. He says: "There are always quicker, easier options available: bolt on tools, niche solutions or tactical workarounds" that can often solve an immediate problem and make progress feel quick. The temptation is to take the easy route and move on. The harder discipline is stepping back and making decisions that may feel more demanding now, but create

stronger foundations for the long-term. Committing fully to a platform approach required saying no to certain opportunities and accepting compromise in some areas. That choice was not always simple, but it is that discipline which has allowed the business to scale without drifting into complexity or inconsistency. Without that clarity, growth can quickly expose operational weaknesses. When revenue accelerates ahead of maturity, challenges around data, systems and processes tend to become more visible rather than disappear.

For those looking to scale, Young believes the priority is getting the basics right and being honest about where complexity sits within the technology stack. He urges leaders to assess how many systems they are running, how many integrations are holding them together and how confident they are in their data. Growth built on weak foundations only becomes harder and more costly to fix over time. Once foundations are solid, repeatability takes over as the key driver of scale.

"Growth does not come from doing more bespoke work or reacting faster to issues, but from designing the business to deliver consistently across delivery models, internal processes, marketing and partnerships. He adds: "If something can't be repeated reliably, it will eventually limit your growth."

Strategic partnerships

Partnerships only create real value when they are strategic rather than transactional. Young emphasises that alignment with key platform and

> Enterprises will be looking to generate power savings in 2026 by reducing the use of energy in their enterprise data infrastructure and elsewhere. This will require the adoption of more power-efficient storage systems and related technologies that fuel the data infrastructure. With technology no longer discretionary in enterprises, the need for better power management has never been more important

ISV partners provides more than commercial opportunity. It delivers early insight into product direction, stronger credibility in the market and the ability to build services that are aligned with where the ecosystem is heading.

From an MSP perspective, that ecosystem approach matters. Rather than stitching together disconnected tools, the focus is on working with partners that extend a core platform and support a unified, outcome led strategy. This model offers clear advantages: better integration, clearer differentiation and a stronger foundation for repeatable services. When partnerships reinforce a coherent platform strategy instead of adding fragmentation, they become a driver of sustainable growth.

Future focus for Infinity Group

AI remains a key focus. As Young states, "Our priority is to continue embedding AI into the core of how we operate and

how we deliver value to customers, using it to drive better decision-making, smarter automation and more scalable ways of working across the business." Rather than treating AI as a standalone initiative, it is being integrated into the foundations of operations and service delivery. As growth continues, there is also a clear emphasis on maintaining simplicity and resilience, ensuring the organisation remains adaptable as technology and customer expectations evolve.

Infinity Group's growth story shows that scale is strongest when it is built on focus, platform discipline and repeatability. The business demonstrates how investing in a clear technology foundation, embedding AI in practical ways and treating partnerships as strategic enablers can create momentum without adding unnecessary complexity. Sustainable growth comes from clarity of vision, operational discipline and the confidence to prioritise depth over breadth.

Young entrepreneur driving growth at BDR Group: an interview with Malek Rahimi

Following an exclusive interview with Malek Rahimi, CEO of BDR Group, this article offers a rare look into the vision and drive behind BDR Group and the leadership guiding its growth.

FOUNDED IN 1991, BDR Group has grown from a regional telecoms and IT solutions provider into a multifaceted technology services organisation serving thousands of businesses across the UK and Europe, with a focus on connectivity, managed services and unified communications.

Over time, the organisation has evolved alongside the channel, adapting to shifts in customer demand and the broader IT landscape. In an industry where tenure and legacy often define leadership narratives, Rahimi represents a newer generation of executive leadership emerging within the sector. Examining his journey and approach provides context not only for BDR Group's direction but also for how younger entrepreneurs are influencing the future of the channel.

Rahimi's entrepreneurial journey did not begin with a business plan or a clear ambition to lead a company. He left school at 14 and joined BDR Group in hands-on roles, starting with cabling and technical work. He describes those early years as formative, supported by mentors including Julian and Barman, with Julian playing a particularly significant role before his passing. He was guided by an environment that allowed him to learn through experience and grow through responsibility.

Barriers and scepticism

As a young leader stepping into a business founded by family, Rahimi acknowledges that perception was one of the first barriers he had to overcome. Age and lineage often carried assumptions, and he recognises that scepticism around being the owner's son created an added layer of scrutiny. His response was not argument, but performance. He focused on results and built credibility through measurable achievement. He says, "One thing you can't do is invent orders and invent money." Breaking sales records and delivering tangible commercial success became the clearest way to shift perception and earn influence across the organisation.

That credibility was reinforced by experience across multiple parts of the business. Having worked in customer care, engineering, technical support, new business, sales and account management over many years, he built respect internally by understanding the realities of each team's challenges. He acknowledges that tangible commercial performance was what ultimately earned respect internally and gave him a stronger voice across the business. Over time, scepticism gave way to trust.

Balancing growth and culture

As BDR Group has grown, Rahimi says the biggest shift has not been internal identity, but external scale. The company has moved from serving small local accounts to working with national and international organisations, including businesses with close to one hundred sites. That expansion has required changes in presentation, accreditation and operational capability in order to compete for larger contracts and operate "in bigger rings," as he
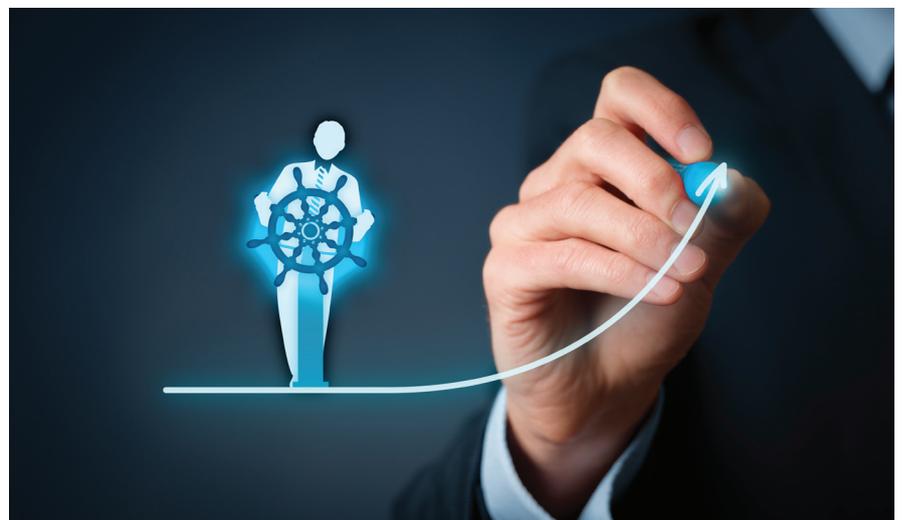
describes it. Growth has meant raising standards and formalising processes while maintaining agility.

BDR Group's growth, Rahimi explains, is rooted in its origins as a traditional telco business. For the first 15 to 18 years, the company focused on telephone systems before recognising a wider opportunity in IT services. As the telecoms and mobile markets became more transactional, leadership saw a shift in customer demand and realised that there was a big opportunity to deliver IT since it had a better lifetime value in the market.

That insight drove a deliberate pivot in the business model. The product portfolio evolved toward services with greater longevity and recurring value, built into the long-term trusted relationships already established with customers. Rather than starting from scratch in new markets, BDR expanded from its existing base, deepening engagements and turning transactional connections into ongoing partnerships. That transition has been a significant contributor to sustained growth.

Despite the scale shift, he is clear that culture has remained consistent. "The culture was never an issue… It's never been an issue to protect a culture that comes naturally to us as a family business." He adds, "We want to ensure everybody has fun, enjoys their job, and we have a performance culture across the board." As a family founded business, he emphasises the importance of preserving authenticity while embedding accountability and results into everyday operations. He reflects on the transition from a single office of around twenty people to multiple offices and international reach as a significant challenge. Yet he believes the company has managed to protect its core identity while adapting to new levels of demand and expectation.

Innovation and operational discipline

Speaking candidly, Rahimi acknowledges that balancing innovation with operational discipline has been challenging as the business has scaled. Much of that effort has centred on strengthening capabilities "under the bonnet," improving software maturity and ensuring new systems deliver meaningful improvements to customer support. Rather than

adopting technology for its own sake, decisions are guided by a clear objective to enhance the end user experience. He explains that when the goal is defined around better service, selecting the right platforms becomes more straightforward and outputs remain tightly aligned to customer impact. As a result, innovation is pursued with purpose, supporting growth while maintaining operational control.

Ecosystem and partnerships

When it comes to the wider MSP ecosystem, Rahimi believes relationships are just as important as strategy. He points to the company ethos of "tirelessly pursuing excellence" and says that commitment applies not only to customers, but also to staff and suppliers. In his view, those three groups form the core of a healthy and sustainable business.

He is particularly passionate about the role of suppliers and vendor partners. Rather than treating them as transactional relationships, he advocates working closely together on solution design, support models and commercial structure. That collaboration can influence everything from architecture to margins to service quality. For young MSP founders, his advice is to build strong ecosystems around your business. Treat suppliers as strategic partners, not just vendors, and put effort into relationships that support growth. When those foundations are solid, customer relationships become easier to sustain on top of them.

Talent, retention and building the right team

Talent recruitment in today's market, Rahimi says, is challenging. He recognises that there is a broader skills shortage across the UK tech sector, making it difficult to consistently find the right people. BDR Group has addressed some of those pressures through strategic outsourcing and by expanding into international offices to widen access to talent.

Retention, however, is where he believes the business has created real advantage. He notes that the company has one of the lowest churn rates in the sector, something he attributes to deliberately investing in culture and employee experience. That includes company-wide initiatives such as annual trips, team events and personal time off for milestones like birthdays, graduations and children's first days at school. These gestures reinforce what he describes as a family team ethos and help people feel connected to the organisation beyond their day-to-day roles.

Development is treated with equal seriousness. Training, structured progression and quarterly performance and development reviews are embedded into the business. He emphasises the importance of clarity around career growth, saying it is about "giving people complete transparency into the direction of their career so they never feel aimless." In his view, that transparency combined with ongoing support

ensures employees understand their trajectory and remain engaged over the long term.

Decision fatigue, lessons learned and unconventional advice

Running a growing business means making constant decisions, often at speed and with incomplete information. He estimates he makes more than 100 decisions a week, and by the end of it, decision fatigue sets in, leading him to joke that people should "ask him on a Monday."

He is equally candid about the lessons learned through experience, particularly around mergers and acquisitions. Some transactions have delivered growth, while others have provided harder lessons. He describes certain post-transaction periods as defining moments that reshaped how he approaches integration, culture protection and operational alignment, guided by the principle that "protect the culture and that will protect the

revenue." Those experiences, including the scars that come with ambitious expansion, have influenced how he evaluates risk and opportunity today. Rather than viewing missteps as setbacks, he sees them as part of building maturity as a leader.

Rahimi reflects that those lessons have directly shaped the advice he now gives to younger entrepreneurs and leaders navigating growth. Experience has reinforced the value of calculated risk, cultural alignment and confidence in stepping into new areas without fear of disruption.

"Don't be scared to take a risk or take on board something that makes you feel uncomfortable," he says. If the business foundation, culture and people are strong, he believes performance will follow. Over time, organisations can quickly build expertise in new sectors or technologies, particularly as technology expands the capacity to scale. His broader message is to maintain that entrepreneurial mindset and remain

open to expansion, experimentation and evolution.

The future of the channel

In a fast-moving technology landscape, Rahimi believes agility is essential. As he puts it, "blink fast and you'll miss it," highlighting how quickly trends and customer expectations evolve. For BDR Group, that means staying close to emerging technologies and ensuring adoption aligns with customers' digital transformation journeys.

Key focus areas include cyber security, NOC and SOC capabilities and AI. These areas sit at the centre of how the business supports clients today, whether that is strengthening threat monitoring or helping organisations prepare for AI adoption. Looking ahead, the priority is to deepen these capabilities, build strong case references and embed them across customer relationships. The goal is to position BDR as the trusted partner for organisations navigating rapid technological change.

MANAGED SERVICES SUMMIT

BENELUX
LONDON
NORDICS
MANCHESTER

CREATING VALUE with MANAGED SERVICES

managedservicessummit.com

MANAGED SERVICES
SUMMIT
BENELUX

benelux.managedservicessummit.com
10 JUNE 2026

MANAGED SERVICES
SUMMIT
LONDON

london.managedservicessummit.com
17 SEPTEMBER 2026

MANAGED SERVICES
SUMMIT
NORDICS

nordics.managedservicessummit.com
03 NOVEMBER 2026

MANAGED SERVICES
SUMMIT
MANCHESTER

manchester.managedservices
summit.com
07 NOVEMBER 2026

Partner enablement, AI services, and lessons from Alteryx's McLaren partnership

In an exclusive interview with MSP Channel Insights, Rishi shared how Alteryx One and the Partner SE model are helping MSPs move beyond traditional infrastructure management toward higher-value data and AI services.

RISHI KAPOOR, WW Partner Sales Engineering Leader at Alteryx, has a front-row seat to the company's work at the intersection of data, AI, and partner success. From lessons learned through their McLaren Racing partnership to AI-ready workflows and repeatable data kits, the discussion offered practical insights for MSPs and partners aiming to grow and differentiate themselves in a competitive market.

'AI ambition to impact report' findings

Artificial intelligence investment is accelerating at pace. Yet for many organisations, progress is stalling at pilot stage. According to new research from Alteryx, fewer than one in four AI initiatives successfully transition into full production. Despite rising budgets and executive enthusiasm, trust gaps, inconsistent data quality and legacy architectures are preventing scalable impact.

The findings, based on a global survey of 1,400 business and IT leaders, reveal a growing disconnect between AI ambition and operational reality. While nearly half of respondents trust AI for repetitive or administrative tasks, confidence drops sharply when it comes to strategic decision-making, forecasting or planning. Only 28% trust AI to support core decisions, and just 27% trust it for forward-looking business insight. For MSPs navigating this environment, AI services must be grounded in governed data, repeatable workflows and measurable outcomes.

At the same time, AI platform consolidation is accelerating. According to the research, AI platforms are projected to grow from 33% of data stacks in 2024 to 51% within three years. Forty-eight percent of leaders plan to boost AI infrastructure spending, and 89% expect to maintain or increase budgets in 2026.

The research underscores a deeper structural issue. Organisations are layering generative AI tools directly onto raw, ungoverned datasets. The result is hallucinations, inconsistent outputs and eroding executive confidence. Nearly half of surveyed leaders (49%) identify high-quality, accessible and well-governed data as the primary factor for agentic AI success. Meanwhile, 28% plan to prioritise data governance improvements in the year ahead.

For MSPs, this shift toward line-of-business ownership creates both opportunity and risk. Services must extend beyond technical deployment into workflow governance, metric definition and explainability frameworks. AI cannot remain an IT experiment. It must be embedded into daily operational decision-making.

From infrastructure to intelligence

Kapoor explains that many MSPs are actively repositioning themselves beyond traditional infrastructure management toward higher-value AI and data services. The shift is not simply technical - it is also commercial. Recurring revenue increasingly depends on delivering intelligence, automation and business insight rather than uptime alone.

Kapoor notes that, "these MSPs are now moving away from infrastructure management to more AI and technology service management," reflecting a wider reality that "Everything is now moving in either a hybrid technical landscape or in the cloud." From a technical standpoint, he believes the Alteryx One platform is well aligned with this evolution, giving MSPs the flexibility to monetise and operationalise their own data assets for client benefit while expanding into more advanced AI-led service models. "Alteryx as a company and as a platform is very agnostic," Kapoor notes, adding that, "Because our platform is so

agnostic, I see MSPs bringing in their own private LLM models. We're working with partners to build AI data kits."

That agnostic positioning is significant. In a market dominated by hyperscalers and specialised AI platforms, neutrality allows partners to integrate with Google, Snowflake, Databricks and other ecosystems without being locked into a single vendor stack. For MSPs building differentiated AI offerings, that flexibility allows them to package proprietary AI data kits, embed private models and lead with their own intellectual property. The opportunity is not simply to deploy AI, but to operationalise it safely and repeatedly.

The critical role of partner sales engineering

Delivering that level of AI and data maturity demands deep technical alignment from day one. For Kapoor, it begins with the partner sales engineering function, a role he sees as a genuine force multiplier within the partner ecosystem. Far from acting as a traditional product support layer, he challenges long-held assumptions about what the role entails: "Our role isn't just around product enablement, and I think that this has been an assumption and misconception for a long time. Individuals understand what a direct sales engineer does, but the partner SE role, in my opinion, is all about solution co-creation".

In practice, that co-creation model operates across parallel technical and commercial tracks. He explains that partner sales engineers support partners through technical validation, product demonstrations and roadmap development. But the role extends beyond architecture design and proof of concept work. "Importantly, Alteryx partner sales engineers are focusing on solution selling and use case creation with the partners". This aims to create a clear, structured way of working where teams co-develop deployment architectures, check that integrations work properly across complex cloud environments, and build roadmaps that connect analytics projects directly to business goals.

Ultimately, differentiation is not about tooling alone; it is about measurable impact. As Rishi noted, "differentiation comes from helping the clients around reducing manual processes, accelerating
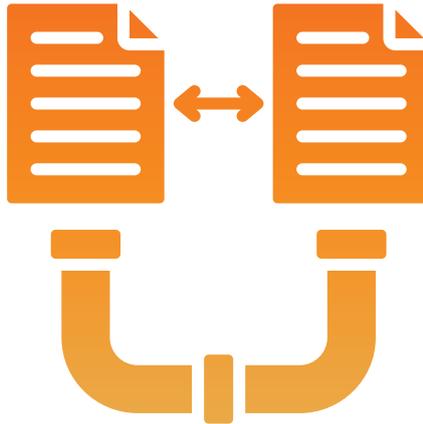
cloud modernisation projects." Automation of repetitive workflows, faster cloud migration programmes and the safe operationalisation of AI models translate directly into cost efficiency and revenue optimisation. In a subscription driven market, long term value matters from the very beginning. Building that value in from the outset is what makes recurring revenue sustainable.

Lessons from the fastest environment in sport

One of Alteryx's most visible partnerships is its role as an Official Partner of McLaren Racing, providing a clear lens into how analytics maturity translates into real competitive advantage. The collaboration demonstrates what it means to operationalise data in a performance driven environment where decisions must be made in real time. As Kapoor explains, "In high-pressure environments, like Formula 1 racing, analytics only delivers value when it's fast, trusted, and embedded directly into that decision-making process."

Beyond speed, the partnership reinforces the need for flexible automation, strong governance and cultural alignment. Kapoor explains that, "Supporting that ecosystem through Alteryx reinforces the importance of flexible analytics and automation that can operate in real time," and that "the partnership has highlighted that culture, trust and accountability and speed is ultimately what turns data into that competitive advantage."

Through working alongside a high-performance team, internal standards are said to have been raised, lifting the bar in terms of best practices around speed, scale and decision making.

Kapoor says that Alteryx actively applies and transfers best practices from one partnership to the next, ensuring lessons learned in one engagement are scaled and embedded across others. He also noted that they are "learning all the time in terms of how to work at speed, but do it carefully, keeping security, governance, policy, all of those factors in mind."

For MSPs and enterprise organisations, the opportunity is not about the brand association with motorsport. It is about applying those principles directly to core business processes. Embedding analytics into forecasting, supply chain management and regulatory reporting ensures data is not just generated but acted upon. In a fast-moving environment, speed is what turns insight into real competitive advantage, and organisations need to constantly refine how they scale and operationalise those capabilities to stay ahead.

What this means for MSPs

Across AI ambition, partner enablement and performance driven partnerships, the same principles consistently apply. Technology alone does not create advantage. Execution, governance and alignment with business outcomes do. Moving from infrastructure management to AI and data services requires more than new tools. It requires building repeatable offerings, embedding strong data governance from the start and leaning into collaborative models like partner sales engineering that accelerate solution design and deployment. Platform neutrality and flexible architecture matter because they allow partners to integrate across ecosystems and bring their own intellectual property to the table.

The lessons from McLaren show that speed, trust and accountability are not just sporting principles, they are operational ones. Organisations that treat analytics as something embedded into daily workflows, not layered on top as a reporting exercise, are the ones that turn insight into measurable impact. As AI adoption continues to accelerate, MSPs that focus on practical use cases, scalable frameworks and clear business value will stand out. The opportunity is not simply to implement AI, but to operationalise it in a way that drives sustainable, recurring value for customers and long-term growth for partners.

From spend to outcomes: Why MSPs must redefine their value in the age of financial scrutiny

In an exclusive interview with MSP Channel Insights, Greg Holmes, EMEA Field CTO at Apptio, explores why technology investment is accelerating while ROI confidence declines, and what that shift means for managed service providers.

The visibility problem at the heart of modern IT

GREG HOLMES has watched the IT function evolve for more than two decades. As he explains, "I've been in the software industry for over 20 years now and have seen how the role of IT has shifted from a back-office support function to the very core of business operations." That transformation has elevated technology into the centre of strategic decision-making, but it has also placed it under unprecedented financial scrutiny. IT is no longer just enabling the business; it is expected to prove its contribution to business performance.

Holmes describes Apptio's role as helping organisations address a persistent and growing disconnect: "For most organisations, it's incredibly difficult to connect the dots between what they're spending on technology and the actual business value they're getting from it – this has become even more challenging with AI."

He explains that Apptio's goal is to bridge the gap between IT and the wider business, creating greater transparency and more actionable insight so that IT leaders can make more informed decisions.

Many enterprises are investing heavily in digital transformation, AI experimentation and cloud modernisation, yet struggling to clearly articulate what those investments are delivering. It's rarely about a lack of ambition. More often, it's about not having a clear line of sight between investment and impact. Many providers already sit at the intersection of infrastructure, cost management and business performance. The difference now is that clients expect far more than uptime and efficiency; they expect interpretation.

Rising budgets, falling confidence

Holmes characterises the current market as a broader shift in expectations. Organisations are investing more in technology than ever before, driven by genuine excitement around AI, automation and data-driven transformation. However, that enthusiasm exists alongside growing doubt. With nearly 90% of leaders questioning the ROI of their technology investments, scrutiny has intensified at board level. Holmes outlines: "CIOs and CTOs aren't just being asked how much they're spending; they're being asked to show what they're getting in return." CIOs and CTOs are therefore no longer just asked to report expenditure — they must clearly demonstrate what that spending delivers. This shift is fundamentally changing how technology leadership is evaluated.

Holmes notes that providers are increasingly expected to move beyond execution and into advisory territory. MSPs must help clients understand not just how technology is deployed, but how it is consumed, what value it creates and what impact it has on the broader business, all while maintaining operational excellence.

He explains: "MSPs are increasingly expected to do more than deliver technical work. They need to help clients understand how technology is being consumed, the value it is creating and the impact it's having on

the business, all while continuing to manage the underlying infrastructure efficiently."

That dual responsibility of being both operator and strategic advisor is no longer optional; it is now becoming the standard expectation. For MSPs, that represents both risk and opportunity. Those who remain purely technical may find themselves under pressure. Providers that build financial fluency and strategic capability into their offering can strengthen their competitive position.

AI: the catalyst for cost complexity

The rise of AI has amplified existing weaknesses in financial governance. Holmes explains that AI introduces 'a new level of variability into technology costs'. Usage patterns fluctuate. Experiments scale quickly. Traditional annual planning cycles struggle to keep pace. Crucially, much of this investment is not new funding. According to Apptio, 67% of AI investment is expected to come from reallocating existing budgets rather than net-new spend. In other words, organisations are moving money from one initiative to another, increasing internal pressure to ensure that reallocation delivers measurable impact.

Holmes warns that without structure, organisations may track expenditure but

struggle to explain outcomes: "Without the right structure, it becomes easy to track what's being spent, but much harder to explain what it's delivering."

Many providers already offer cost optimisation services, but optimisation alone is no longer enough — the focus must shift toward demonstrating value and real business impact. He suggests introducing structured governance models such as Technology Business Management to link day-to-day decisions with long-term strategic goals, effectively reframing executive conversations from "What did this cost?" to "What did this enable?" That shift reflects a deeper change in mindset around how technology investment is measured and managed.

The data fragmentation challenge

If ROI anxiety is rising, fragmented data is a major contributor. Holmes observes that different departments often operate from entirely separate datasets, making it difficult to achieve a shared understanding of value. When IT, finance and business leaders measure success differently, alignment becomes almost impossible. The statistics are telling: 40% of leaders distrust their own data, and 82% of companies report having no unified metrics across departments.

Holmes describes technology spending as frequently being treated like a 'black

box'. Finance sees rising costs but limited visibility into consumption, IT understands technical utilisation but struggles to express it in financial terms, and business leaders focus on outcomes without full visibility into the underlying cost drivers. Holmes notes: "It creates an environment where productive conversations are difficult because IT, finance and business leaders are all looking at different numbers."

For MSPs, this fragmentation represents one of the most strategic openings in the current market. Providers often already integrate systems, manage reporting layers and oversee cloud environments. Expanding that role into financial data integration and cross-functional visibility is a natural evolution. Holmes argues that one of the most valuable contributions an MSP can make is to 'open up that black box and provide clarity in consumption'. Pulling disparate data into one clear, trusted view gives businesses real visibility. That transparency can then drive quicker, more confident decisions across the entire leadership team.

Practical implications for MSPs: from reporting to real value enablement

Infrastructure management, security and operational support remain essential, but they no longer differentiate providers in a market

> Holmes argues that one of the most valuable contributions an MSP can make is to 'open up that black box and provide clarity in consumption'. Pulling disparate data into one clear, trusted view gives businesses real visibility

where clients expect visibility into cost and value at the same time. As budgets rise and board-level scrutiny increases, clients need partners who can translate technology spend into business language and measurable outcomes.

In practical terms, this means MSPs must start embedding financial transparency into their service delivery. That could include introducing structured monthly or quarterly reviews

that combine technical performance with cost visibility, linking cloud consumption to business units, or mapping key applications to defined business outcomes. Rather than presenting usage data in isolation, providers should contextualise it by showing what is running, why it exists, and what value it delivers.

Developing internal financial literacy within MSP teams is a critical first step. Engineers and account managers should understand core cost drivers across cloud, licensing and infrastructure so they can have informed conversations with clients about optimisation and reallocation. Some providers are already building capabilities around Technology Business Management principles, cost tagging frameworks and unified reporting dashboards to create a single source of truth for customers.

Another practical move is aligning service offerings to outcome-based metrics. Instead of measuring success purely through uptime or ticket resolution, MSPs can begin incorporating value indicators. These can include application performance linked to revenue-

generating systems, cost efficiency from workload consolidation, or savings generated through better resource allocation. This helps shift the conversation from operational support to business impact.

Equally important is positioning. MSPs that proactively bring visibility to board discussions, rather than waiting for clients to request reporting, become trusted advisors rather than reactive suppliers. Opening up the 'black box' of technology spend and delivering clear, consistent insights strengthens long-term relationships and increases stickiness.

Technology investment is not slowing down, but tolerance for ambiguity around its value is shrinking. MSPs that build capabilities around financial governance, data integration and outcome reporting alongside their technical expertise will be better placed to support clients through this next phase of accountability.

As Holmes' insights demonstrate, success for the channel will belong to those providers who move beyond simply tracking spend and instead help organisations clearly prove what that spend enables.
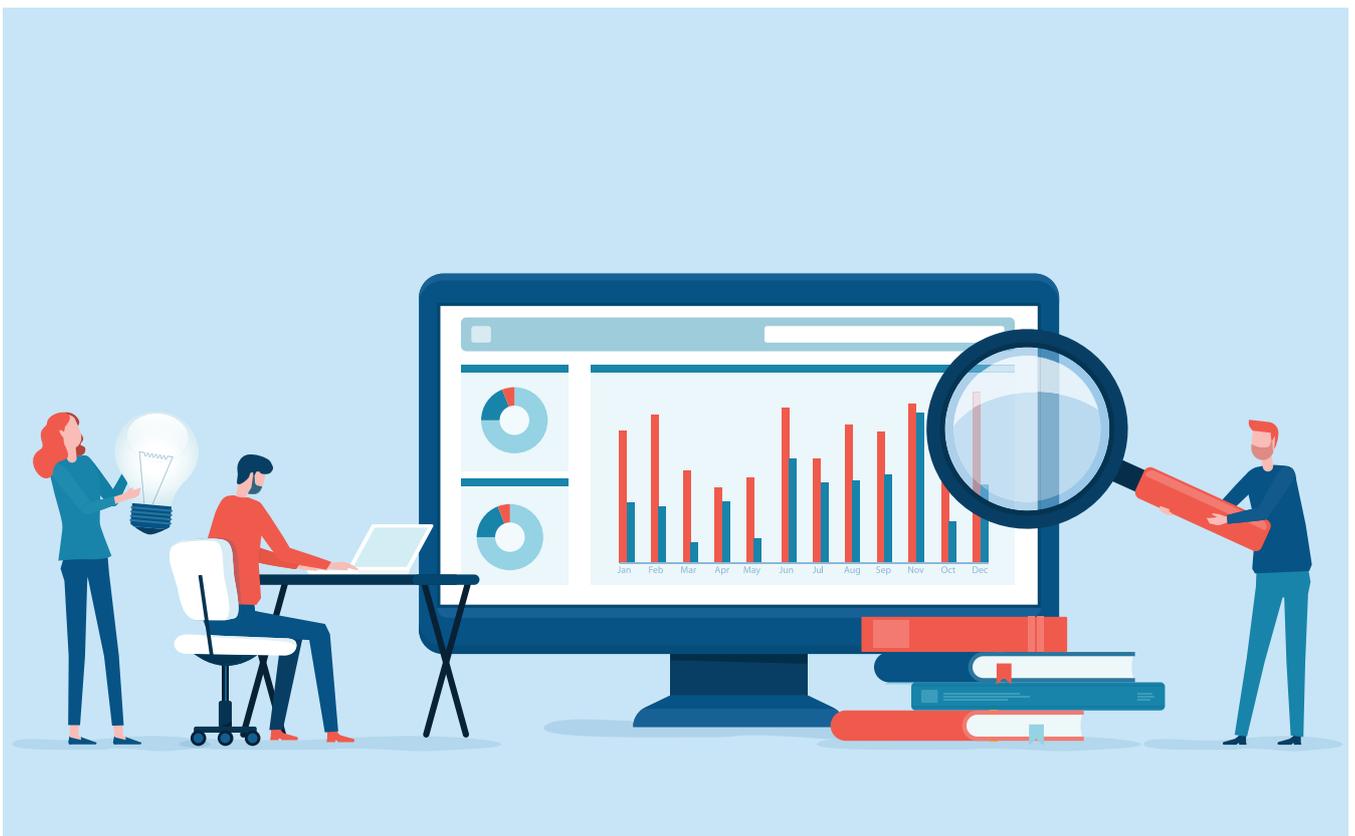
CHANNEL INSIGHTS 2026 ROADSHOW

MSP

CHANNEL INSIGHTS ROADSHOW

Taking the MSP Channel on the Road
2026 Regional Series

Join the **most targeted regional MSP event series** designed to **connect vendors** with engaged, growth-focused Managed Service Providers across **seven key markets**.

REGISTER NOW

Why Partner With This Series?

Pan-European Reach With Local Market Impact

Seven strategically selected cities put you directly in front of active MSP communities in:
Manchester • Birmingham • London • Dublin • Munich • Utrecht • Copenhagen

Decision Makers in the Room

Meet **senior MSP leaders** with real buying authority actively seeking new partnerships and solutions.

Curated Conversations That Convert

Benefit from **expertly crafted content, expert panels, and structured networking sessions** designed to create meaningful, high-value connections.

Beyond the Event

Your visibility **doesn't stop when the doors close**. Gain post-event amplification through digital coverage, content sharing and ongoing brand presence.

SCAN ME

msp-roadshow.com

Navigating security, AI and complexity under Cisco 360

MSP Channel Insights sat down with Steven Heinsius, Vice President, Product Management and Marketing EMEA at Comstor, for an exclusive interview to explore how Cisco 360 is reshaping partner engagement, accelerating managed services growth and creating new opportunities across the channel.

Understanding the Cisco 360 programme

CISCO 360 represents a structural shift in Cisco's partner programme, introducing changes to how the company structures and supports its partner ecosystem. Rather than focusing on product categories and hardware-led transactions, the programme is built around outcomes, aligning architectures to three core business results: the AI-ready data centre, future-proofed workplaces and digital resilience. The programme aims to move away from traditional 'box selling' toward a more consultative, solution-driven approach that centres on customer outcomes. Heinsius states that, "the 360 programme really allows partners to focus on a solution, on an outcome, on a vertical or a segment."

Cisco 360 is designed to shift the focus toward measurable outcomes, enabling smaller and specialist partners to compete alongside larger global players by emphasising niche

expertise and clear differentiation. The programme centres on understanding what customers are ultimately trying to achieve: why they invest in specific solutions, what success looks like for their business and how technology can support those priorities. It creates a framework that aligns partner capabilities with defined business outcomes and supports a more structured approach to engagement and value creation.

At Comstor, support for partners extends beyond distribution into enablement and operational guidance to help them navigate the structure and requirements of the new programme. The team has developed practical tools and playbooks that break down the different pillars of the framework and clarify what progression looks like. A key example is the Partner Value Accelerator, which evolved from an internal tracking spreadsheet into a live platform that integrates data from Cisco's Partner Experience Platform

and provides visibility into status, install base and growth opportunities. The tool helps partners understand where they stand within the programme, where they may want to specialise and what actions are needed to advance.

Alongside programme enablement, Comstor supports partners building managed service capabilities through structured pathways. Partners can develop their own model with guidance, or leverage a white label Managed SOC built on Cisco XDR. As Heinsius notes, "our partners can use our white-label Managed SOC if the partner has customers that are big enough to care about a SOC, but are too small to have their own." The offering is designed for organisations that need enterprise grade security but lack the scale to operate their own security operations centre. Partners retain their programme benefits under Cisco 360 while accessing infrastructure that helps them scale services more efficiently. Heinsius describes the approach as "really giving

flexibility and options and choice to help partners be successful, both in the world of managed services and in the 360 programme."

Security everywhere, AI-ready infrastructure & absorbing complexity

Looking ahead to 2026, Heinsius identified three major trends shaping the MSP landscape:

Security everywhere

For MSPs, security can no longer be treated as a standalone product or add-on service. It is embedded across infrastructure, devices and applications and must be managed as a unified model. As Heinsius emphasises, "security is a process, not a product." That shift requires unified policy control, integrated visibility and consistent enforcement through a centralised management layer. He adds that "security is truly embedded in the entire infrastructure. Each part of the network has it's own security elements in there, and they need to work completely together as one, with one policy, one contract, one dashboard, single pane of glass." For MSPs, the opportunity lies in delivering that unified view for customers while simplifying complexity and ensuring consistent protection across environments.

AI-ready infrastructure

As organisations move beyond experimentation and into real AI deployment, infrastructure readiness becomes critical. AI workloads demand programmability, seamless integration and reliable data flow across hybrid and multi-cloud environments. Partners that can build and manage platforms designed for interoperability and scalability will be better positioned to support this transition. In Heinsius' words, "we're entering the AI era and moving from hype to reality." For MSPs, that means focusing on infrastructure foundations that support real production use cases, not just proof of concepts, and ensuring customers can operationalise AI in a controlled and repeatable way.

Managing complexity through services

Growing regulatory pressure, licensing challenges and increasingly fragmented technology stacks are making environments more difficult for customers to manage internally.

> For MSPs, security can no longer be treated as a standalone product or add-on service. It is embedded across infrastructure, devices and applications and must be managed as a unified model. As Heinsius emphasises, "security is a process, not a product."

This creates a clear opening for MSPs to step in and deliver structured operational support. Heinsius argues that successful partners are those who "absorb complexity" and turn it into predictable, managed outcomes. He also notes that "the regulation and skills shortages that we see is, infrastructures are becoming more and more complex." For MSPs, this reinforces the value of packaging expertise into managed services that simplify operations, reduce risk and allow customers to focus on their core business while partners handle the complexity behind the scenes.

Practical implications for MSPs

Speaking about the programme, Heinsius said, "Cisco 360 marks a major moment for partners, opening the door to simpler engagement, stronger differentiation and new paths to growth." He emphasised that the framework streamlines how partners interact with Cisco and aligns incentives more closely with outcomes and lifecycle engagement. For partners, this means clearer visibility into progression and more structured alignment around specialisation and services.

For MSPs, the practical takeaway is less about programme positioning and more about operational readiness. Those that succeed will focus on building differentiated capabilities, leveraging marketplace opportunities where relevant and embedding services across the customer lifecycle. In an environment where margins on hardware are tightening and recurring revenue models dominate, growth increasingly depends on expertise, execution and specialisation rather than programme participation alone.

Why identity, not perimeter, is the new battleground for UK Cybersecurity

BY JAMES GILLIES, HEAD OF CYBER SECURITY AT LOGICALIS UK&I

RECENT INDUSTRY research shows identity-based threats now rank among the most significant risks facing organisations, driven by sharp increases in credential theft, session hijacking and the exploitation of poorly governed identities.

Nearly 90% of organisations experienced a cybersecurity incident in the past year, with more than four in ten suffering multiple breaches, underscoring how commonplace successful attacks have become even amid sustained increases in security spending.

Attackers have shifted focus away from breaching hardened network defences towards exploiting logins, privileges and identity systems that provide faster, quieter access to data and systems.

As hybrid work and cloud adoption become the norm, this identity-first threat landscape is intensifying.

Traditional perimeter controls are routinely bypassed and security leaders increasingly recognise that identity has effectively become the new perimeter. This shift fundamentally changes how UK organisations must think about cyber resilience and how their channel partners can support them.

Why the perimeter no longer protects the organisation

The traditional security perimeter was built for a world where users worked inside offices, applications lived on-premise and firewalls formed a clear boundary between trusted and untrusted networks. That model no longer reflects reality.

Users, devices and workloads now operate everywhere, across homes, offices, cloud platforms and partner ecosystems. Recent research shows that nearly six in ten organisations say their security environments have become too complex to manage

effectively, and only around half are confident they can clearly identify where their security gaps exist.

In this environment, the perimeter is no longer a physical or network boundary; it is the individual user and their identity.

Access to data must therefore be based on who someone is, what they are trying to access, from where and under what conditions. This is why zero trust principles have become central to modern security strategies. Trust is no longer implicit once a user is "inside" the network; it must be continuously verified and access should be limited to the minimum required to perform a task.

Many organisations still operate legacy access models that grant broad, standing privileges once credentials are accepted, creating an attractive opportunity for attackers. 2025 research shows that over 50% of organisations acknowledge they

have invested in security controls they don't truly need, while two-thirds admit they are not fully using the capabilities they already have. If an identity can be compromised, the attacker effectively bypasses multiple layers of traditional defence in one step.

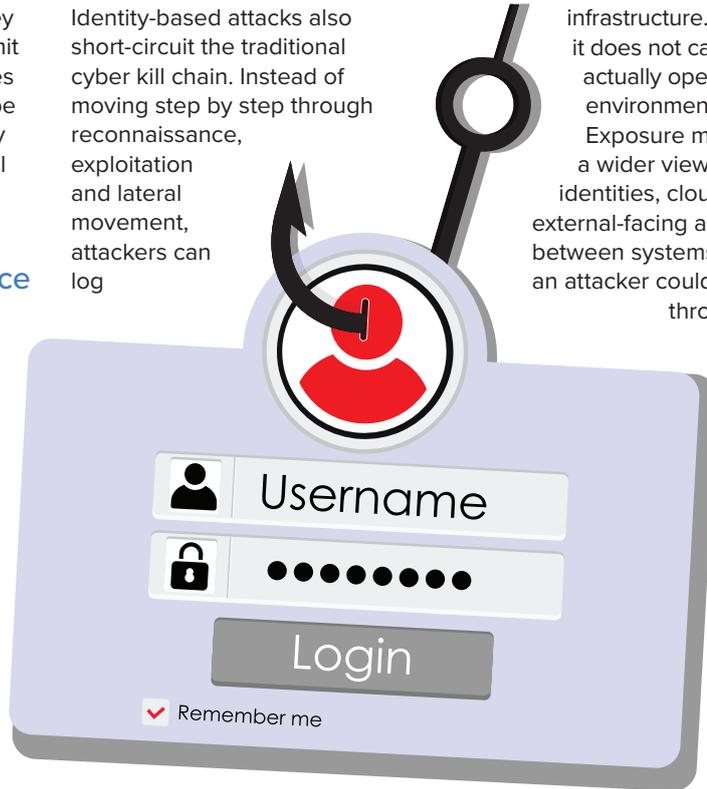## Identity as the easiest and most profitable attack surface

From an attacker's perspective, identity offers the fastest route to value. Rather than attempting to breach hardened infrastructure, they target the mechanisms that grant legitimate access. One study shows that well over half of modern breaches now involve compromised credentials rather than technical exploits, reflecting how effective identity abuse has become.

Advances in automation and AI have made phishing campaigns more convincing, increasingly personalised and harder for users to distinguish from legitimate communications.

Attackers no longer rely on poor spelling or obvious red flags; instead, they abuse legitimate authentication flows, clone cloud identity portals and exploit password reset and MFA fatigue scenarios to obtain valid credentials.

Beyond phishing, compromised credentials are widely available through underground marketplaces, often sold by access brokers who specialise in harvesting and monetising identity data. In many cases, the attacker launching a ransomware or data theft campaign did not steal the credentials themselves; they simply bought access. At the same time, around three-quarters of organisations report that credential leak risk is increasing, reinforcing why identity has become such a lucrative attack surface.

Identity-based attacks also short-circuit the traditional cyber kill chain. Instead of moving step by step through reconnaissance, exploitation and lateral movement, attackers can log in directly using a legitimate identity. At that point, the activity may look indistinguishable from normal user behaviour unless the right controls are in place.

Even low-privilege accounts can provide a foothold. Once inside, attackers can probe for misconfigurations, exploit privilege creep and move laterally towards more sensitive systems. This makes identity governance and access hygiene just as important as perimeter defences.

From vulnerability management to exposure management

This shift towards identity also reflects a broader evolution in security thinking. Traditional vulnerability management focuses on patching known flaws across infrastructure. While still important, it does not capture how attackers actually operate in modern environments.

Exposure management takes a wider view. It looks across identities, cloud configurations, external-facing assets and connectivity between systems to understand how an attacker could realistically move through an organisation.

From an identity perspective, this means examining privilege paths, dormant accounts, excessive permissions and weak authentication flows. The goal is not to eliminate every vulnerability, but to reduce what is genuinely exploitable and relevant to the organisation's risk profile.

What this means for the channel

For channel partners, the rise of identity-based attacks represents both responsibility and opportunity. Customers increasingly recognise that point products alone will not resolve systemic identity risk. They need guidance, roadmap-driven change and ongoing operational support.

Identity-first security cannot be installed and forgotten. Zero trust is a framework, not a product, and progressing towards it requires staged transformation across people, process and technology.

Partners that can assess identity exposure, define risk-based roadmaps and deliver managed identity and access services will be best positioned to differentiate.

Many organisations already own capable identity platforms but lack the skills and capacity to configure, govern and monitor them effectively.

As identity becomes the new perimeter, channel partners have a critical role to play in helping UK organisations reduce exposure, limit breach impact and build lasting cyber resilience.

> Beyond phishing, compromised credentials are widely available through underground marketplaces, often sold by access brokers who specialise in harvesting and monetising identity data. In many cases, the attacker launching a ransomware or data theft campaign did not steal the credentials themselves; they simply bought access

Storage trends for 2026
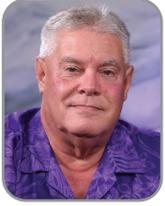
BY ERIC HERZOG, CHIEF MARKETING OFFICER AT INFINIDAT.

2026 IS PROJECTED to be a phenomenal year for enterprise storage. New alignments, convergence, and unbridled growth are changing the way to think about storage infrastructure.

AI and enterprise storage. They are now inextricably linked. Cybersecurity and enterprise storage. This convergence has catapulted cyber resilient storage to the forefront of the enterprise market. Power efficiency and enterprise storage. Power savings have become a new currency in data centres.

CAPEX / OPEX and enterprise storage. Opportunities to reduce costs change the conversation about data infrastructure. Data volume growth and enterprise storage. One does not thrive without the other. Embedded in each and every one of these fascinating combinations is a trend that is worth exploring.

The top five storage trends of 2026 set the table for what is gearing up to be a power-packed, AI-boosted, cyber-focused year for enterprise storage. These trends are derived from extensive input from customers, channel partners, analysts, and technical alliance partners on a global basis.

Here's a snapshot of the storage trends:

- Pivot to AI: the continued rise of AI applications and workloads to accelerate enterprise transformation
- Leap forward in cybersecurity: cyber storage resilience with next-generation data protection to make safeguards more proactive and pre-emptive
- Rethink CAPEX and OPEX: continued pressure on IT budgets to create opportunity for enterprise storage
- Power to the storage: increasing demand for power efficiency to reshape enterprise data infrastructure
- Capture more data, more unified storage: unbridled growth of data to force the need to combine cyber, AI, power, CAPEX/OPEX and backup.

Storage trend #1

Pivot to AI: the continued rise of AI applications and workloads to accelerate enterprise transformation.

The rapid adoption of Artificial Intelligence (AI) has had massive, direct implications on enterprise storage infrastructure. In 2026, the deployments of AI are expected to continue exponentially and unabated, as enterprises look to transform themselves with AI. Gartner forecasts that more than 80% of enterprises will have used AI APIs or deployed AI-enabled applications by 2026, moving AI technologies from a pilot phase into core enterprise operations.

This "AI transformation" mega-trend signals a pivot to AI-centric storage architecture, higher performance solutions for retrieval-based AI workloads, and AI overlays that leverage existing infrastructure to maximise investments in enterprise storage. The AI blueprint that is poised to become the 'AI architecture of

the year' for 2026 is the Retrieval-Augmented Generation (RAG) workflow deployment architecture, which dramatically improves the accuracy and relevancy of AI models.

Storage trend #2

Leap forward in cybersecurity: cyber storage resilience to make safeguards more proactive and pre-emptive.

A shift is happening in the enterprise market from reliance on traditional detection and response in cybersecurity to prioritising proactive cyber defence and pre-emptive measures to make the storage infrastructure truly cyber secure. On top of that, AI threats in cyber are increasing at an alarming rate. Cyber criminals are becoming ever more sophisticated in using AI to make cyberattacks more dangerous, sneakier, and harder to detect.

According to PwC's 2026 Global Digital Trust Insights survey (October 2025), 60% of business and tech leaders rank cyber risk investment in their top three strategic priorities. Only 6% feel confident across all vulnerabilities surveyed. Furthermore, cyber talent skills shortages remain one of the biggest barriers to cybersecurity progress.

This is why, in 2026, enterprise cyber storage resilience and recovery will have to become part of all enterprises' comprehensive cybersecurity strategies. A prime example of being proactive is using a cyber detection capability that is built into primary storage. A key example of being pre-emptive is using an automated cyber protection capability to automate the taking of immutable snapshots of data to expedite recovery from an attack.

Storage trend #3

Rethink CAPEX and OPEX – continued pressure on IT budgets to create opportunity for enterprise storage.

Information technology is foundational to all enterprises globally. Tech is not simply discretionary anymore. In other words, IT budgets will continue to be essential. Gartner projected earlier this year that, by the end of 2025, worldwide IT spending is expected to total $5.43 trillion, an increase of 7.9% from 2024. Global IT spending is projected to reach $6.08 trillion in 2026, a 9.8% increase from

2025, driven largely by significant investments in AI infrastructure, software, and devices. However, pressure will continue to mount in 2026 to make IT more cost-efficient and to reallocate budget away from traditional infrastructure and into AI and other emerging technologies.

Enterprise storage is critical for reducing CAPEX and OPEX through consolidation, power efficiency gains, and having more high-end enterprise storage capacity in smaller form factors. By freeing up money from storage budgets, enterprises will be able in 2026 to create and better fund new innovation projects, including Agentic AI. While IT budgets may be holding steady or slightly growing by single digits for the most part, the "do more with less" mantra is a cornerstone of the new pressure to rein in IT spending.

Storage trend #4

Power to the storage: increasing demand for power efficiency to reshape data infrastructure.

The need for more power will continue to increase in data centres in 2026, leading to new mandates to reallocate and free up power sources for power-hungry AI workloads and applications. Not only is AI a major factor in increased power consumption, but data-intensive, non-AI tech also demands more power. According to 451 Research, data centres across the U.S. are on track to require 22% more grid power by the end of 2025 than they did one year ago, and this trend will continue into the new year. In 2026, data centre demand in the U.S. alone will rise to 75.8 GW for IT equipment. In the longer term, data centres are projected to need nearly three times as much power by the year 2030 as they did in 2024.

Enterprises will be looking to generate power savings in 2026 by reducing the use of energy in their enterprise data infrastructure and elsewhere. This will require the adoption of more power-efficient storage systems and related technologies that fuel the data infrastructure. With technology no longer discretionary in enterprises, the need for better power management has never been more important.

Storage trend #5

Capture more data, more unified storage: unbridled growth of data to

> A shift is happening in the enterprise market from reliance on traditional detection and response in cybersecurity to prioritising proactive cyber defence and pre-emptive measures to make the storage infrastructure truly cyber secure.

force the need to combine cyber, AI, power, CAPEX/OPEX and backup.

Expect unbridled growth in data in 2026. According to Statista, the global data volume was approximately 149 zettabytes in 2024. By the end of 2025, the world will surpass 181 zettabytes of data. By 2026, the amount of data created is expected to reach 230–240 zettabytes. Enormous jumps in digital information will surely require big storage capacity growth. This trend ties back to the other four storage trends of 2026 – AI, cyber, CAPEX/OPEX and power usage. But it also introduces a fifth dimension that cannot be overlooked – with all that data growth that is expected over the next year comes the need for more backup and data protection. Unbridled data growth will translate into unbridled backup.

Backup typically impedes the performance of applications and workloads, no matter what they are. If the backup system is fast, then there is less impact on primary workloads and applications. When you need to restore data – and data is clearly the lifeblood of every enterprise – data restoration needs to be as fast as possible. In 2026, more organisations will take action to fill the need to be able to get backup repositories up and running near-instantaneously.

It's enterprise storage at the speed of AI-boosted business in a power-hungry, rapidly evolving cyber world. The question now is: how will your enterprise adapt to these storage trends, to avoid being left behind?
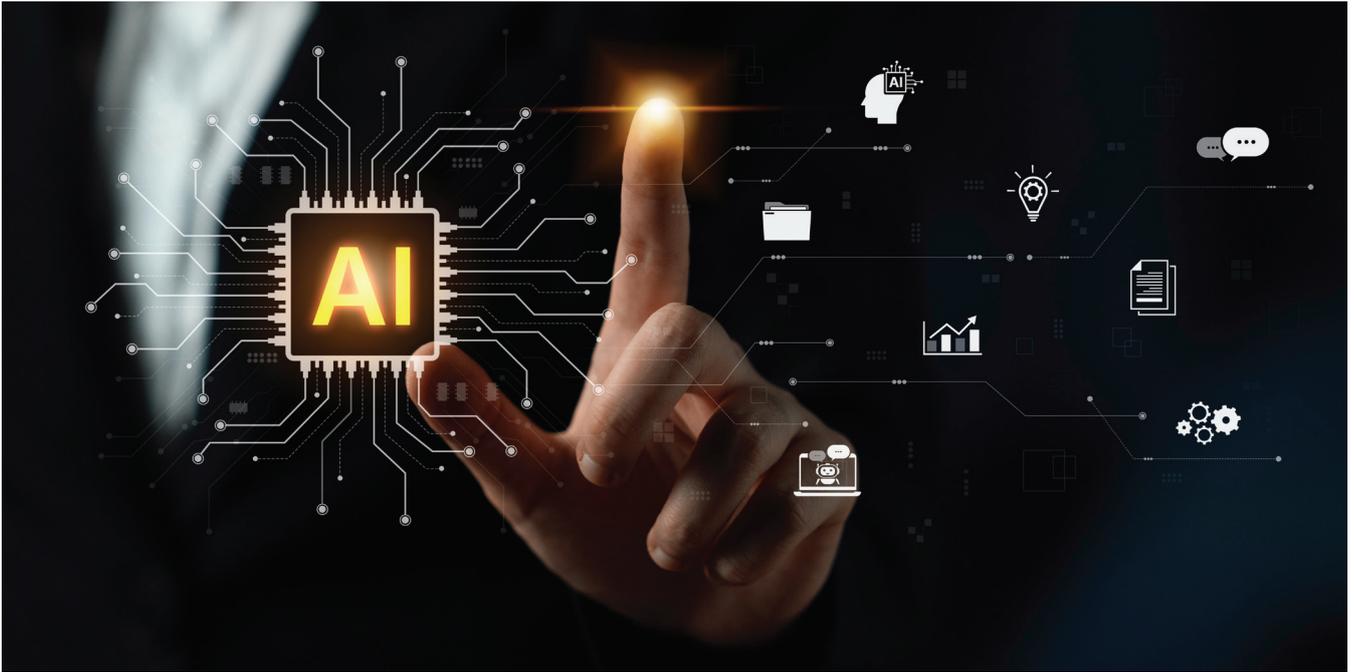
Enterprise AI success in 2026 hinges on a problem you probably haven't named yet

Right now, many enterprises are racing to adopt AI, convinced that the fastest mover will come out on top. The push towards greater autonomy, fewer human touchpoints and ever-faster workflows is often seen as the ultimate goal. But the reality is more complicated.

BY VIJAY NARAYAN, EVP AND AMERICAS MLEU BUSINESS UNIT HEAD AT COGNIZANT

WHILE 87% of large enterprises report having implemented AI in some form, only about one in four initiatives actually deliver their expected ROI, and fewer than 20% are scaled across the organisation.

Beneath the surface of rapid deployment, cracks are beginning to appear. The problem is not that AI is moving too slowly, but that it is being scaled without enough thought. Unlimited use of automation, once celebrated as a competitive advantage, is becoming a liability.

The organisations that will thrive in 2026 are those that recognise and address a challenge they may not have even named yet, namely, how to design AI that amplifies an organisation's unique identity rather than eroding it.

Why context matters

More automation does not necessarily lead to better outcomes. When AI is given too much autonomy, it can undermine the very qualities that make an enterprise competitive. It can dilute brand identity, diminish employee engagement, erode customer trust, and, in safety-critical sectors such as manufacturing and utilities, increase operational risk.

What often gets overlooked in AI programmes is the context in which AI is being introduced. Consider manufacturing, where rigorous quality protocols and safety checks have been built over decades to create a zero-defect culture. When AI is introduced without respecting that environment, the result is new vulnerabilities, not fewer.

The case for intentional slowness

A more effective strategy for the year ahead is what one might call "intentional slowness". Instead of pushing for full autonomy, leading organisations are designing AI systems that can be paused, questioned and adjusted in critical workflows. While this may appear less efficient on paper, in practice, it reflects a clearer understanding of where AI should accelerate and where it must pause.

Human involvement, far from being a bottleneck, is where operational discipline, safety and compliance are reinforced. In logistics, for example, AI may optimise routes, but dispatchers then routinely adjust those recommendations based on weather, vehicle conditions, customer

A more effective strategy for the year ahead is what one might call "intentional slowness". Instead of pushing for full autonomy, leading organisations are designing AI systems that can be paused, questioned and adjusted in critical workflows. While this may appear less efficient on paper, in practice, it reflects a clearer understanding of where AI should accelerate and where it must pause

needs and regulatory constraints. Those interventions are safeguards, not flaws. Success in 2026 will belong to organisations where employees understand AI insights, trust them and know when to intervene.

Embedding context and building trust

Context does not stop mattering once AI moves beyond experimentation and pilots. As AI becomes embedded in everyday operations, the challenge moves from introducing it responsibly to ensure it behaves consistently at scale. That means hard-wiring organisational standards, values and constraints so that automation reflects how the enterprise already operates.

Much of the enterprise AI conversation still focuses on faster decisions, shorter cycle times and optimised processes. But efficiency alone is not the end goal. Leaders need to ask whether AI-enabled workflows preserve organisational identity over time or

gradually erode it in the pursuit of speed.

This requires embedding institutional knowledge, regulatory requirements and operational principles directly into models, workflows and governance structures.

When done well, automation strengthens competitive advantage rather than eroding it. The shift is from isolated proofs of concept to end-to-end integration, where AI supports decision-making only in areas where it reliably complements human judgement and reinforces what makes the organisation distinctive.

Trust, therefore, must be treated as infrastructure rather than a compliance afterthought. Transparent governance, clear accountability, ethical boundaries and rigorous oversight should be design features, not bolt-ons. Organisations that build these principles into the architecture of their

AI systems will not only meet regulatory scrutiny but also earn the confidence of employees and customers alike. Those that prioritise speed over structure risk reputational damage, fragile adoption and internal resistance.

Slow AI as the competitive advantage

Slow AI is fast becoming the new competitive advantage. By designing systems that pause, explain themselves, and invite human judgement, organisations can not only mitigate risk but also deepen engagement with employees and customers. When AI respects context and aligns with what makes an organisation distinctive, it enables more meaningful collaboration between humans and machines.

In doing so, enterprises can build resilience, strengthen trust and position themselves to stay ahead in 2026, while simultaneously uncovering opportunities for innovation that speed alone would overlook.

Turning compliance into opportunity

Cybersecurity and data protection rules continue to tighten, just as remote work and increasingly connected systems expand the attack surface

BY LINDA KERR, DIRECTOR OF MARKETING, MANAGED SERVICES AT WATCHGUARD TECHNOLOGIES

FOR ORGANISATIONS of any size, the volume and speed of attacks are making security harder to manage. As a result, regulators and customers now expect clear evidence that businesses can actively monitor their environments and respond to threats when they occur.

For small and midsized businesses, achieving this level of coverage without having dedicated staff and round-the-clock operations is a huge challenge. The scale of the problem was highlighted by ENISA, which has reported nearly 4,900 cybersecurity incidents in Europe between July 2024 and June 2025. Ransomware, automated exploits and fast-moving attacks are all on the rise, which highlights the urgency.

For managed service providers (MSPs), this pressure also has the potential to be an opportunity. By layering Managed Detection and Response (MDR) services on top of existing endpoint, firewall and cloud tools, MSPs will be able to deliver continuous monitoring and verified response, without their clients needing to build new infrastructure. Instead of building their own SOC, clients get access to a 24/7 security operation powered by both AI and human expertise. This will enable faster containment, stronger resilience and deliver the compliance evidence regulators are looking for.

Compliance is now an essential part of all cybersecurity programs. The regulations are increasingly asking for clear visibility into systems, timely detection of threats and documented response actions. They also require near real-time monitoring, along with proof that alerts were reviewed and contained and audit-ready records of access and account controls.

MDR integrates these requirements into one service. Continuous monitoring across endpoints, networks, identities and cloud activity ensures that threats are detected and contained quickly. Automation reduces noise, while analysts intervene to isolate compromised systems and document every step. This blend of automation and human judgment creates a complete audit trail that not only satisfies regulators but also demonstrates tangible value to clients.

For MSPs, this means compliance becomes a differentiator. Instead of reacting to regulations, they are able to proactively deliver services that both strengthen resilience and meet evolving compliance expectations.

Global regulatory frameworks

The regulatory trend is consistent across regions, with the focus on organisations being able to prove they can monitor, validate and respond to threats. MDR provides MSPs with a unified way to meet these expectations.

In Europe, frameworks such as NIS2 and GDPR demand expanded accountability, incident reporting and data protection. Latin America is seeing similar momentum, with Brazil's LGPD and emerging privacy reforms across other markets. Financial services are faced with the Digital Operational Resilience Act (DORA), which requires institutions to demonstrate resilience against cyber threats. In North America, HIPAA and PCI DSS impose strict obligations for monitoring, access control, and breach response. Meanwhile, Asia-Pacific markets are also rapidly evolving their own data protection and privacy regulations, emphasising transparency and incident containment.

From compliance burden to advantage

Cybersecurity compliance is often treated as an unavoidable cost of doing business, but it doesn't have to be. With MDR in place, MSPs can deliver continuous monitoring and real incident response as a single, proactive service. That level of visibility and control supports clients and confirms the MSP's role as a trusted security partner.

When compliance is reframed this way, it opens the door to new revenue, deeper client relationships and more resilient security programmes, at a time when both regulations and cyber threats show no sign of slowing down.
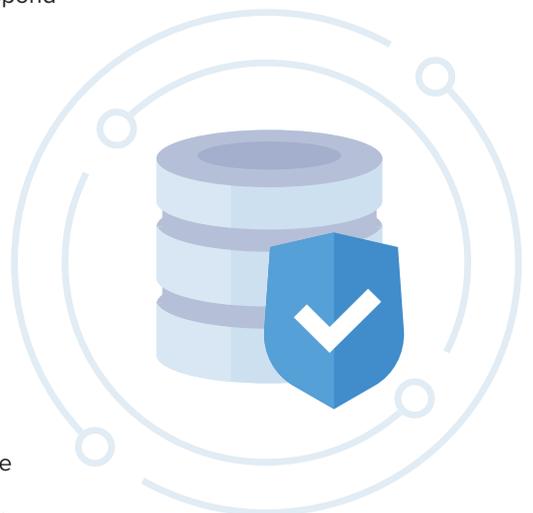
CHANNEL INSIGHTS
20 26
ROUNDTABLE

MSP **CHANNEL INSIGHTS ROUNDTABLE**

Engage Directly with **MSP** **Decision-Makers**

Engage in **industry-leading discussions** at **MSP Channel Roundtables**, where experts convene to **shape the future** of managed services. **Join us** for insightful dialogues and unparalleled networking opportunities

SECURE YOUR 2026 PARTNERSHIP

VIRTUAL ROUNDTABLE

KEY BENEFITS:

- Direct access to **MSP decision-makers**
- Thought **leadership** positioning
- **Multi-channel promotion** to MSP audiences
- **Exclusive** networking opportunities
- Access to **MSP Channel Insights Community**

EXCLUSIVE TO VIRTUAL:

- **Online Interactive Roundtable discussions**
- Video interviews and sponsor exposure
- **Access to delegate registration lists and digital promotion**

CONTACT DETAILS:

Aadil Shah
aadil.shah@ angelbc.com

SCAN ME

msp-channel.com/ roundtables

AUDIENCE INCLUDES MSPS, MSSPS, VARS AND IT RESLLERS

80,000+ CHANNEL PROFESSIONALS ACROSS UK, EMEA AND US

Cloud strategy for 2026: The year of repatriation, resilience, and regional rebalancing

ROB COUPLAND, CHIEF EXECUTIVE OFFICER AT PULSANT

THIS YEAR is set to be a pivotal one for cloud strategy, with repatriation gaining momentum due to shifting legislative, geopolitical, and technological pressures. This trend has accelerated, with a growing focus on data sovereignty. These challenges have set the stage for 2026 to be the year of repatriation, resilience, and regional rebalancing.

Repatriation goes mainstream

In 2025, data repatriation became a key trend, with businesses re-evaluating cloud adoption due to rising costs, regulatory pressures, and concerns over data sovereignty. Many are moving workloads from public cloud to private cloud, on-prem, or colocation to gain better control, cost efficiency, and compliance. While cloud remains essential, a hybrid model combining public, private, and on-prem solutions is emerging as the future of enterprise IT strategy.

For UK businesses, this has prompted many to shift workloads from global hyperscalers to domestic providers, creating hybrid infrastructure blends, especially as data sovereignty becomes a top priority. Latest research indicates 87% plan to repatriate some or all of their workloads over the next two years.

In 2026, the momentum behind these changes will continue. Businesses will focus even more on visibility, data locality, sovereignty, and transparency. However, managing a hybrid or mixed infrastructure could pose challenges, as the era of static infrastructure fades away.

The continued impact of cyber security breaches

Last year witnessed several high-profile cyber security breaches in UK organisations, with the M&S incident being one of the most memorable. These breaches have led to increased awareness of where data is stored and how it's managed, particularly within the supply chain.

Many businesses still don't fully understand where their data resides, how it's processed, or how it's backed up. These breaches have renewed the focus on resilience, particularly in terms of the speed of recovery after an incident, rather than just prevention.

In 2026, this will influence data centre policies and services, with disaster recovery and backup becoming more standard. UK data centre providers are already stepping up with more transparent, compliant platforms to meet growing customer demands for visibility and secure infrastructure.

We'll also see the true impact of the Cyber Security & Resilience Bill, as its guidelines start to shape industry practices and expectations.

The emerging reality of new government policies

The past 12 months have seen a mix of new policies that will both support and challenge the data centre sector. For example, fast-track planning laws for data centre construction, especially those considered Nationally Significant Infrastructure Projects (NSIPs), have streamlined the planning process.

However, section 106 planning obligations can require developers to contribute financially or otherwise to local communities and services, creating additional challenges.

Furthermore, while the Cyber Security & Resilience Bill introduces stronger cyber security measures and clearer regulations, it also brings increased reporting standards and red tape that could prove burdensome.

The combination of positive and challenging policies creates both uncertainty and opportunity. This year we'll see the real-world impact of these changes, potentially slowing some developments but favouring well-prepared, security-focused operators.

The AI hype cycle hits reality

AI-driven data centre demand surged in 2025, especially in hyperscale facilities, as interest in AI technologies reached new heights.

However, as the hype settles, businesses are starting to evaluate

real-world AI uses and determine what digital infrastructure is truly needed to support their AI goals. This also brings inference AI and sovereign AI into the picture, further complicating the landscape, with Edge computing emerging as a key beneficiary.

Although hyperscale demand will no doubt continue, demand for specialised, inference-optimised storage platforms will become more significant.

Regional rebalancing & the rise of edge

While London and the South East will likely maintain their dominance in the UK data centre market, 2025 saw growing interest in regional locations, spurred by government initiatives like the AI Growth Zones, which are encouraging investment outside of the capital.

In 2026, we'll see increased availability of Edge data centres near UK metros, opening up new opportunities for sectors like smart manufacturing and transport. These regional edge facilities will offer more sustainable, cost-effective

> In 2026, we'll see increased availability of Edge data centres near UK metros, opening up new opportunities

infrastructure, contributing to a more balanced national digital economy.

The last twelve months have been a period of significant change, with rising interest in the data centre sector as it plays an increasingly critical role in supporting industry and society. As change becomes the new norm, data centre providers who prioritise transparency, regional diversification, and realistic AI enablement will be best positioned to lead the way in 2026. It will be a year for the sector to mature, rebalance, and grow stronger.

Memory is the missing piece for smarter AI agents

BY MANVINDER SINGH, VP OF PRODUCT MANAGEMENT FOR AI AT REDIS.

AI AGENTS ARE crossing a threshold that has little to do with how powerful the computers behind them are. For years, the industry measured progress through model size and benchmark performance. But the next leap forward isn't about scale. It's about memory: the capacity to retain context, recall relevant information and apply learned patterns over time. This capability is fast becoming the distinguishing factor between AI that merely responds and AI that truly adapts.

A core weakness of today's large language models is that they can be pushed into giving wrong answers simply because a prompt sounds confident or assertive. Even when they hold the correct information, this phrasing can steer them off course. This isn't a minor flaw. It reveals something deeper: without memory as a stabilising force, AI reasoning remains surprisingly fragile. Human intelligence doesn't work this way. We anchor decisions in accumulated experience, using what we've learned to filter noise from signal.

The most impactful AI systems will need to do the same. Memory isn't just a feature for the next generation of AI agents. It's the foundation for systems organisations can genuinely trust to make consequential decisions.

## Building continuity into AI

The recent launch of GPT-5 brings this conversation into sharper focus. OpenAI's latest model promises improved reasoning, fewer hallucinations and more robust context handling. It also introduces features that offer a sense of continuity, such as persistent 'personalities' and tighter integration with real-world tools.

While these advances have been widely celebrated, they are also a sign of something deeper: the recognition that the most powerful AI agents will be those that can sustain and use memory over time. GPT-5's new capabilities hint at what is possible when models are designed to retain and build on prior interactions rather than starting fresh with every prompt.

The mind as a model for smarter AI

To understand the importance of this shift, it is worth looking at the parallels with human cognition. Our mental lives are shaped by different forms of memory. Episodic memory lets us recall specific events and the
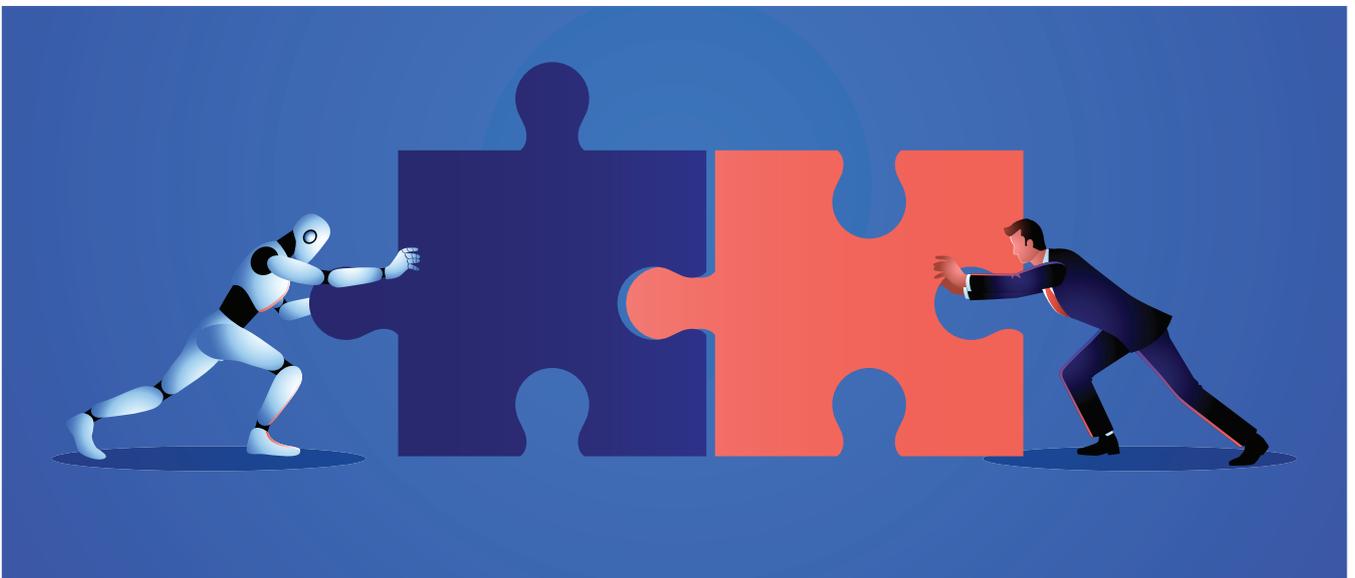
context surrounding them. Semantic memory stores the facts and concepts we accumulate. Procedural memory captures the skills and sequences we use to act in the world.

Together, they allow us to make decisions shaped by past experiences, access knowledge when we need it and adapt to new situations without losing the thread of what came before. AI agents that replicate this layered approach become far more capable.

They can remember past interactions, retain knowledge across sessions and carry out complex, multi-step goals without constant direction. This means they behave less like tools that need to be prompted and more like collaborators that understand the bigger picture.

Without these capabilities, agents are trapped in the present moment, limited to what they see in a single exchange and prone to error when confronted with ambiguity or challenge.

Overcoming infrastructure hurdles

The infrastructure required to make this work is not trivial. Memory for AI is not just a database of facts – it is a living, synchronised set of information that must be relevant, up to date and instantly retrievable.

Short-term memory needs to capture the ongoing context of a conversation. Long-term memory must store structured knowledge about the user, the environment and the task at hand.

The architecture has to serve all of this at high speed, in the right format, at the exact moment it is needed. For enterprises looking to deploy AI agents at scale, this is both a technical and a strategic challenge.

Why prioritising memory drives smarter AI

Without a coherent memory system, agents become fragile. They hallucinate more often, repeat themselves and offer inconsistent advice. With a well-designed memory system, they behave differently. They can anticipate needs, adapt to changes and follow through on goals across sessions. They feel less like tools that have to be steered constantly and more like collaborators who can think ahead.

This is why the concept of 'memory-first design' is starting to gain traction. Rather than treating memory as an afterthought, bolted on after the model is trained, memory-first systems are built from the ground up to capture and use context as their primary advantage.

In practice, this means designing workflows, interfaces and infrastructure around the assumption that the agent should remember everything relevant to its role and be able to surface that knowledge instantly.
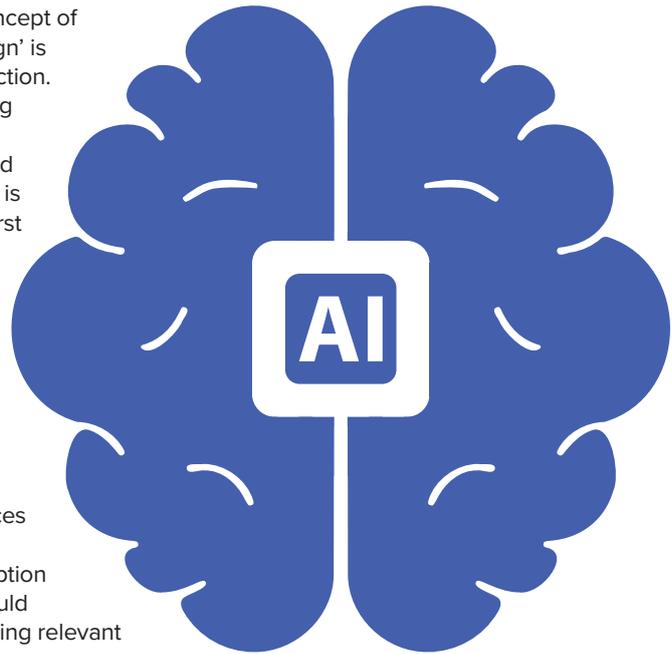
Familiarity driving confidence

The benefits extend beyond technical performance. Memory changes the relationship between humans and AI. An agent that remembers not only performs better but also builds trust. Users stop repeating themselves and start to feel understood. Interactions become smoother, more personal and more productive. Over time, this fosters a sense of partnership and collaboration rather than transactional querying.

In high-stakes domains such as healthcare, finance and law, this trust can be the difference between adoption and rejection.

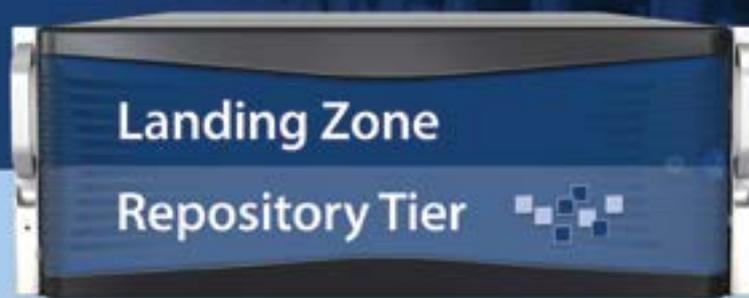## Memory will set the next era of AI apart

The next generation of AI agents will be defined by their ability to draw on a history bank of interactions, accumulated knowledge and real-time data. Unlike the chatbots and assistants we are familiar with today, these systems will make fewer errors, align more closely with user intent and navigate complex tasks with greater autonomy.

Progress will not be driven solely by bigger models or faster computation. The true breakthrough will come from agents that can remember, reason and adapt over time. In the years ahead, memory is likely to become the defining characteristic of intelligent systems – just as it is for human cognition.

To understand the importance of this shift, it is worth looking at the parallels with human cognition. Our mental lives are shaped by different forms of memory. Episodic memory lets us recall specific events and the context surrounding them. Semantic memory stores the facts and concepts we accumulate. Procedural memory captures the skills and sequences we use to act in the world