MSP CHANNEL INSIGHTS

ISSUE I 2026

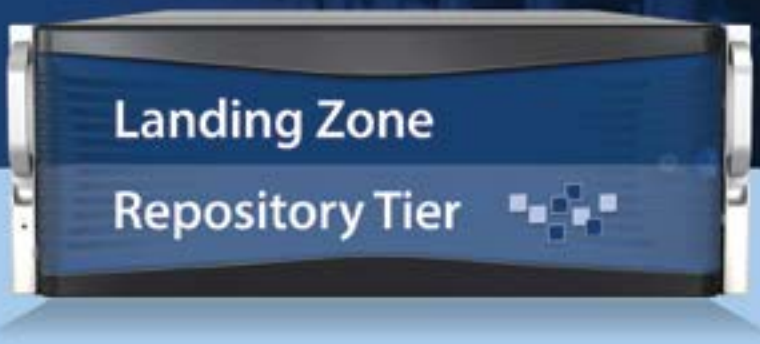
AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

MSP-CHANNEL.COM

CELEBRATE THE WINNERS OF THE 2025 CHANNEL AWARDS

EXAGRID
Tiered Backup Storage

The future is here.
Tiered Backup Storage



FASTEST BACKUPS

FASTEST RESTORES

SCALABILITY FOR FIXED-LENGTH BACKUP WINDOW

COMPREHENSIVE SECURITY WITH RANSOMWARE RECOVERY

LOW COST UP FRONT AND OVER TIME

MSP CHANNEL AWARDS
2025 WINNER

- BACKUP & DR INNOVATION OF THE YEAR
- STORAGE HARDWARE INNOVATION OF THE YEAR
- STORAGE VENDOR OF THE YEAR

Thank you so much to all who voted, and congratulations to our fellow MSP Channel Awards 2025 winners!

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

LEARN MORE >

VIEWPOINT

BY SOPHIE MILBURN
EDITOR

What's Driving the MSP Channel in 2026

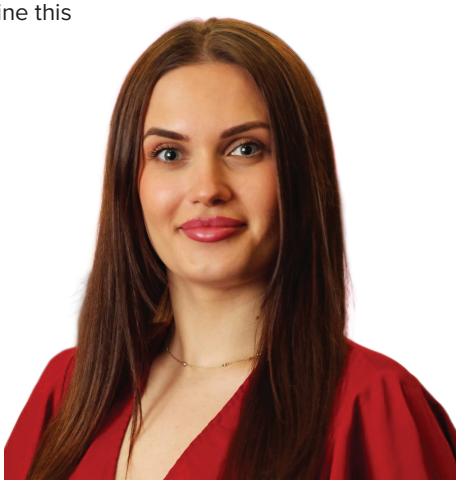
OVER THE PAST MONTH, as the new editor of the MSP Channel Insights portfolio, I've been immersing myself in the channel, speaking with leaders across MSPs, SaaS providers, hyperscalers, and cybersecurity specialists. These conversations, combined with our events like the Manchester 2026 Roadshow, have given me a front-row view of the trends and challenges shaping the channel this year.

What has genuinely surprised me is the positive outlook for the channel in 2026, even in the face of significant challenges. MSPs are navigating the complexities of AI and automation, including integrating agentic AI responsibly, upskilling teams, and balancing operational efficiency with personalised client support. Yet, through these interviews and events, it has become clear that there is a strong sense of optimism and determination across the sector. Industry leaders are focused on innovation, collaboration, and practical strategies to turn challenge into opportunity.

AI and automation are already reshaping operations, from everyday workflows to how identity and security are managed, yet there's a clear focus on embedding these technologies thoughtfully rather than simply reacting to them. It's evident that businesses are under pressure from increasingly sophisticated threats, and many are still navigating how to turn AI into practical, manageable solutions. What stands out is how the sector is leaning into proactive, platform-driven approaches. They are aiming to use automation intelligently, prioritising strong data foundations, and placing identity and security at the centre of their strategy. Watching and listening to how leaders are tackling these issues has shown me a channel that is adaptable, resilient, and future-focused.

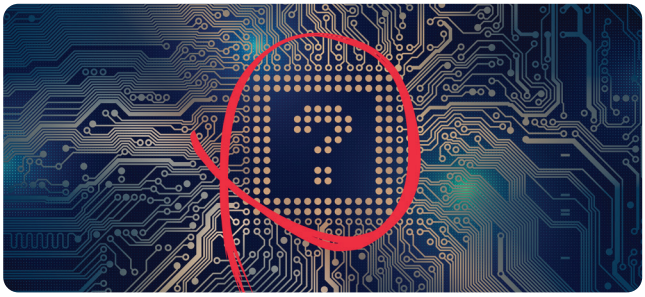
Insights from the broader industry underline these trends. SMBs face escalating AI-driven attacks and identity-based threats, emphasising the need for consolidated, data-led security platforms. Meanwhile, practical adoption of AI continues to be guided by human oversight, governance, and incremental change, showing that technology and people must evolve in tandem.

Engaging with so many voices has highlighted just how dynamic and interconnected the MSP landscape is and reinforced the importance of turning these insights into practical guidance for MSPs as they plan for 2026 and beyond. At MSP Channel Insights, we remain committed to sharing these perspectives, highlighting the strategies, ideas, and voices that will define this transformative year.

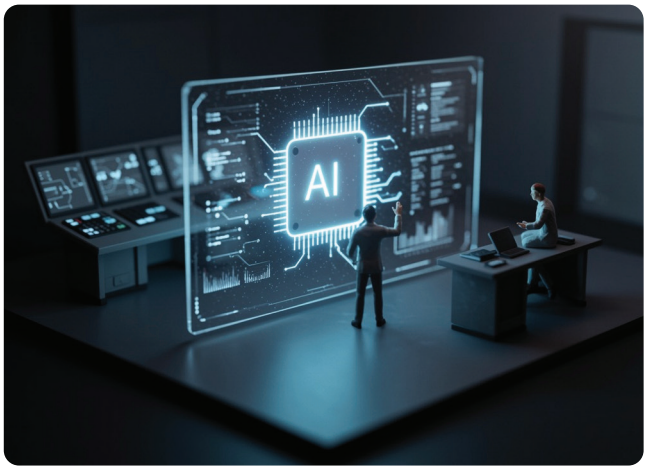


MSP CHANNEL INSIGHTS

Contents



NEWS



MSP CHANNEL INSIGHTS

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

Consulting Editor
Philip Alsop
philip.alsop@angelbc.com

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

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

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

Graphic Design & Multimedia Assistant
Harvey Watkins
harvey.watkins@angelbc.com

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

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

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

Directors
Sukhi Bhadal: CEO
Scott Adams: CTO

Angel BUSINESS COMMUNICATIONS

MSP-Channel Insights is published eight times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication.

ISSN 2396-9016 (Online)

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

F5 elevates API discovery and security with platform enhancements

F5 unveils enhancements to its Application Delivery and Security Platform, advancing API discovery, threat detection, and connectivity in multi-cloud environments.

F5 NETWORKS, an application delivery organisation, recently announced key improvements to its F5 Application Delivery and Security Platform (ADSP). The latest updates focus on enhancing API discovery capabilities, improving threat detection, and optimising network connectivity.

These updates aim to strengthen F5's ability to provide unified visibility and operational efficiencies across diverse cloud environments.

The enhancements are included in the newly launched 7.0 release of F5 Distributed Cloud Services. This update reinforces visibility and control to protect APIs, indicating F5's continuous innovation in cloud services and their growing significance within the F5 ADSP framework.

Broader platform enhancements aim to offer:

- Expanded API Discovery: Customers now have broader options to visualise hidden endpoints and data flows across varied environments, including BIG-IP and NGINX, without needing to redesign applications or network paths.
- Improved API Testing and Threat Detection: F5 has enhanced testing to address more API vulnerabilities, providing enhanced detection for critical threats. This supports organisations in maintaining high-level security in complex ecosystems.
- Strengthened Bot Defence: F5 has enhanced integration of Bot Defence with its managed services, facilitating an easier onboarding process with automated policy applications. Organisations can modify control policies swiftly to adapt to emerging threats.
- Operational Enhancements for Cloud-Native Environments: The release introduces a modernised service discovery framework for Kubernetes and Consul, enabling efficient mapping of services to tenants with role-based control.
- Advanced Networking Enhancements: F5 Distributed Cloud Network Connect now offers expanded routing intelligence, integrating third-party networking solutions, strengthening connectivity and traffic management.

With these comprehensive updates, F5 enhances its platform strategy, ensuring its Distributed Cloud Services remain a critical component of cloud security and connectivity strategies.

Cybersecurity services expand into North America

INTEGRITY360 has announced its acquisition of Advantus360, a Canadian cybersecurity services and solutions provider based in Calgary. Although the exact terms of the transaction remain undisclosed, this move is part of Integrity360's ongoing global expansion, establishing a presence in North America.

Advantus360, founded in 2015, offers a range of services to diverse clients across Canada and the United States, particularly in the oil, gas, and energy sectors, alongside transportation, manufacturing, and several other industries.

The firm operates in various domains of cybersecurity consulting such as design, architecture, assessment, and remediation, alongside integration and deployment. It also provides strategic development and training. Advantus360 has worked with Palo Alto Networks and holds related accreditations. Additionally, it has partnerships with other vendors, including Cisco and Mimecast.

By becoming part of Integrity360, Advantus360 is set to evolve into a regional hub covering Canada and the broader US market, an important step in Integrity360's vision.

This will include the opening of a new Security Operations Centre (SOC) in Calgary by 2026, serving as a local site for Integrity360's SOC operations, which are currently located in various cities in Europe and Africa. Additional sites are planned for Brussels and Paris.

Advantus360's clientele hope to gain enhanced access to Integrity360's cyber services, including risk assurance, round-the-clock incident response, forensic services, and PCI compliance. The managed services offering includes Managed SASE and Comprehensive Threat Exposure Management (CTEM), among other solutions. Integrity360's services have been recognised in the Gartner market guide.

This acquisition aims to strengthen Integrity360's position in global cybersecurity and offer Advantus360 leverage to expand its services further across North America with the backing of a larger infrastructure.

Keepit's channel expansion: partner-first approach

Keepit aims to strengthen its global channel team, focusing on partner-led strategies to drive SaaS data protection globally.

KEEPIT, a cloud-native data protection provider, has announced an expanded global channel organisation, helping demonstrate its commitment to fostering growth through its partnerships. Under the guidance of Jan Ursi, Global Vice President of Channels, the setup is designed to ensure partners remain the focal point of Keepit's market strategies.

The new structure assigns regional oversight for Southern Europe, Northern Europe, and the Americas. This seeks to bring channel expertise and regional insights, aiming to strengthen Keepit's presence and offer consistent yet adaptable support to partners.

Keepit aims to operate through a 100% channel-led market approach, collaborating with value-added resellers, managed service providers, and strategic alliances. The goal: to establish a cohesive global framework that facilitates enablement, joint marketing, and collaborative sales, while granting regions flexibility to cater to local dynamics.

"At Keepit, being partner-friendly isn't just a slogan — it's our culture," Ursi emphasises. The strategy reinforces the company's partner-led approach to SaaS data protection.

Cyril VanAgt leads efforts in Southern Europe and DACH, fostering local ecosystem growth. Emphasis is placed on region-specific campaigns and a structured Partner Academy programme, already piloted in Paris, with plans for further rollout.

In Northern Europe, led by Alex Walsh, the strategy revolves around strengthening key partnerships. A data-driven approach, consistent enablement, and media engagement are considered key to scaling successful collaborations.

Over in the Americas, Jill Miracle ensures the strategic focus remains steady, aiming to leverage Keepit's global Partner Academy tracks to keep partners informed and equipped.

With this global strategy in place, Keepit's channel organisation aspires to scale and grow symbiotically with its partners. The plan includes further partner recruitment, enhancing certifications, and intensifying joint marketing across vital markets. The ultimate goal is to empower partners to build reliable and sustainable SaaS data protection practices.

Lenovo's AI-driven data solutions

Lenovo's new portfolio targets AI and data storage requirements, providing solutions for enterprises seeking to modernise their infrastructure.

LENOVO has revealed a suite of data storage and virtualisation solutions to help enterprises modernise their IT infrastructure. These new offerings – ThinkSystem and ThinkAgile – provide a modern foundation for businesses aiming to achieve AI innovations.

According to industry reports, many organisations are unsure about their data management practices, which greatly influences AI deployment. Lenovo's new solutions integrate hardware, software, and services to harness enterprise data's true potential.

To tackle current AI challenges, a robust data management strategy is key. Lenovo addresses this by focusing on those businesses that require efficiency, flexibility, and scalability in their virtual and physical data environments.

Lenovo's latest offerings include:

- ThinkSystem DS Series Storage Arrays: Designed for virtualised environments, these systems provide enhanced performance by using all-flash technology.
- ThinkAgile FX Series: Offering hyperconverged infrastructure, this provides maximum protection and flexibility through a convertible, open architecture.
- ThinkAgile MX Series: With NVIDIA RTX Pro 6000 integration, the system enhances AI capabilities within Microsoft Azure environments.

These new offerings – ThinkSystem and ThinkAgile – provide a modern foundation for businesses aiming to achieve AI innovations.

- ThinkAgile HX Series: Supports AI deployment through Nutanix Enterprise AI software, optimised for virtualised and containerised environments.

The portfolio's standout feature is the comprehensive range of hybrid cloud and data lifecycle services. These services simplify AI deployment, enhance data management, and support evolving storage needs:

- Lenovo Deployment Services: Accelerating infrastructure rollout for organisations with ThinkAgile and ThinkSystem offerings.
- TruScale Model Solutions: For flexible consumption of storage services, enhancing performance across the data lifecycle.

Long-term strategies are also supported through Lenovo's cloud consultancy and advisory services, ensuring compliance, data protection, and operational efficiency.

With direct access to Lenovo experts, the Premier Enhanced Storage provides professional monitoring and optimisation for critical workloads. Customers can hope to rely on these solutions for maintaining system reliability and supporting innovative AI and hybrid cloud growth.

NinjaOne announces conference for MSPs - MSP NXT

MSP NXT conference in Austin this October will feature insights, collaborations, and actionable strategies specifically designed for MSP growth.

NINJAONE, known for its automated endpoint management solutions, is set to host its inaugural conference, MSP NXT, aimed at managed service providers (MSPs). Scheduled for October 27-29, 2026, the event will be held at the Marriott Austin Downtown and will provide a platform for industry leaders.

The conference will cover a range of topics relevant to the MSP community, focusing on industry innovations, business education, technical training, and collaborative sessions. This initiative aims to support the development and growth of the MSP market.

Paul Redding, Head of MSP Partnerships at NinjaOne, highlighted the event's important role in fostering a supportive environment for MSPs to thrive. He emphasised that the conference would offer a fun, actionable experience, providing MSPs with real conversations, tangible results, and strategies they can immediately implement.

Attendees can look forward to a comprehensive agenda featuring keynote addresses from industry experts, interactive breakout sessions, and hands-on training. These activities are designed to equip MSP leaders with practical insights and action plans to enhance profitability and customer outcomes.

Networking opportunities will be abundant, enabling participants to engage with both peers and prominent industry leaders. This collaborative atmosphere aims to forge relationships that can underpin lasting success in the ever-evolving MSP landscape.

Sal Sferlazza, CEO and co-founder at NinjaOne, expressed the event's significance in uniting the MSP community, providing a platform for shared ideas, and exploring the future of this dynamic industry. He recognised the MSP community's contribution to the event and expressed his eagerness to connect with attendees in Austin.

The conference welcomes leaders and technicians globally. For those interested, further information, updates, and registration details can be accessed through the official channels.

Britain leads Europe in AI adoption, emphasising its positive impact

THE UNITED KINGDOM emerges as a frontrunner in integrating artificial intelligence (AI) into workplace environments, outshining its European peers. According to recent findings from TOPdesk, a global IT service management solutions provider, employees in the UK show an acceptance towards AI, expressing minimal concern about its potential impact on their jobs.

The research indicates that 75% of UK organisations have already embedded AI within their operations. Of these entities, nearly half, accounting for 47%, have achieved measurable benefits from AI utilisation. Contrary to widespread apprehensions about job displacement owing to AI, only a modest 10% of participants feel threatened by AI.

This confidence among the workforce is translating into further action. A substantial 88% of UK IT professionals advocate for increased automation in their daily work processes.

A significant portion of this advancement is propelled by the IT departments, responsible for spearheading AI implementations in 70% of UK enterprises.

These departments are facilitating internally-driven transformations using solutions to enhance productivity, precision, and decision-making.

The exploration further underscores the UK's priority on a positive digital employee experience. Notably, 60% of the participants highlighted their commitment to fostering such an experience, which significantly dwarfs the 26% in the Netherlands and surpasses Germany at 29% and Belgium at 43%.

While the enthusiasm for AI integration remains high, professionals have expressed desires for improved guardrails. Approximately 26% suggest increased training is necessary to empower employees to utilise AI effectively.

Moreover, 37% voiced concerns about data privacy and oversight, emphasising that while the UK champions AI adoption, maintaining a balance through continuous investment and responsible AI use remains pivotal.

Schneider Electric, AVEVA, and ETAP join Alliance for OpenUSD

The Alliance for OpenUSD aims to advance interoperable digital twins, simulation-ready 3D assets, and AI infrastructure, supporting industrial digitalisation and more sustainable energy solutions.

SCHNEIDER ELECTRIC, AVEVA and ETAP have announced their membership in the Alliance for OpenUSD (Universal Scene Description). The companies join NVIDIA, Pixar, Adobe, and Autodesk in helping to shape the future of interoperable digital twins and simulation-ready (SimReady) 3D assets. The announcement was revealed during Schneider Electric's Innovation Summit North America in Las Vegas, convening more than 2,500 industry professionals to discuss practical solutions for a more resilient, affordable and intelligent energy future.

The announcement reinforces the companies' commitment to advancing open standards for industrial simulation, collaborative design, and Gigawatt-scale AI infrastructure. OpenUSD is an extensible framework and ecosystem that supports interoperability between software tools and data types, facilitating the development of virtual environments and industrial digitalisation.

Joining the Alliance signals Schneider Electric, AVEVA, and ETAP's deepened alignment with NVIDIA's vision for scalable, physically accurate, and real-time digital twin environments, engineered to simulate buildings, manufacturing factories, data centres, and AI infrastructure systems of the future.

Organisations are rapidly adopting NVIDIA Omniverse libraries to develop digital twin solutions to model projects, digitalise processes, and design systems to a high standard of performance, sustainability and energy efficiency.

The initiative focuses on advancing open standards for industrial simulation, collaborative design, and AI infrastructure systems.

By adopting OpenUSD as a shared standard, the companies are working closely with NVIDIA to unlock new possibilities for:

- SimReady Asset Development: Creating interoperable, simulation-ready models of physical infrastructure components, like power and cooling systems, that can be orchestrated within industrial digital twins that leverage NVIDIA Omniverse libraries.
- Digital Twin Collaboration: Enabling unified views of complex systems such as data centres, energy grids, and industrial facilities that are integrated with Schneider Electric's platforms like EcoStruxure, AVEVA and ETAP.
- Accelerated AI Infrastructure Deployment: Leveraging the NVIDIA Omniverse DSX Blueprint and NVIDIA Omniverse libraries to codesign gigawatt-scale AI factories with reduced risk and faster time-to-market.

The three companies' multi-domain expertise across buildings, data centres, factories, plants, grids, and infrastructure aims to offer digital twin simulations for an array of industries.

Schneider Electric's SimReady assets are used alongside applications with integrated NVIDIA Omniverse libraries, enabling physically accurate, detailed simulations across industries and accelerating digital twin development. This ranges from manufacturers optimising assembly lines to data centre operators enhancing AI factory design and operations. For example, by using AI factory digital twins, data centre operators can model and manage physical infrastructure systems that simulate thermal behaviour, power distribution, and airflow to optimise cooling efficiency and reliability.

Rev Lebaredian, Vice President of Omniverse and simulation technology at NVIDIA, highlighted that building and running complex systems such as AI factories requires a strong, simulation-ready foundation. He noted that combining Schneider Electric's expertise in energy management and hardware with NVIDIA Omniverse libraries is expected to help speed up the development of AI factories and smart grids, supporting more efficient and sustainable AI-driven operations.

Continued innovation, partnership, and impact: Schneider Electric, AVEVA, and ETAP joining the Alliance marks an important step in the companies' partnership with NVIDIA and builds upon milestones they have achieved to advance digital twin and AI factory development.

The companies are co-developing reference architectures, integrated infrastructure and software solutions that will power and cool the next generation of AI factories, and working on projects that leverage NVIDIA Omniverse libraries to simulate and improve energy efficiency in real-world environments.

At GTC DC, Schneider Electric was named as a power, cooling, and energy technology partner contributing to the NVIDIA AI factory Research Centre in Manassas, Virginia. Powered by the NVIDIA Vera Rubin platform, the centre was built to support enhancements in generative AI, scientific computing and advanced manufacturing and to serve as a foundation for the Omniverse DSX Blueprint for gigascale AI factories. In March 2025, ETAP by Schneider Electric unveiled a digital twin that can accurately design and simulate the power needs of AI factories.

Snowflake acquires Observe for AI-powered observability

Snowflake announces plans to acquire Observe, aiming to enhance its AI Data Cloud with observability solutions.

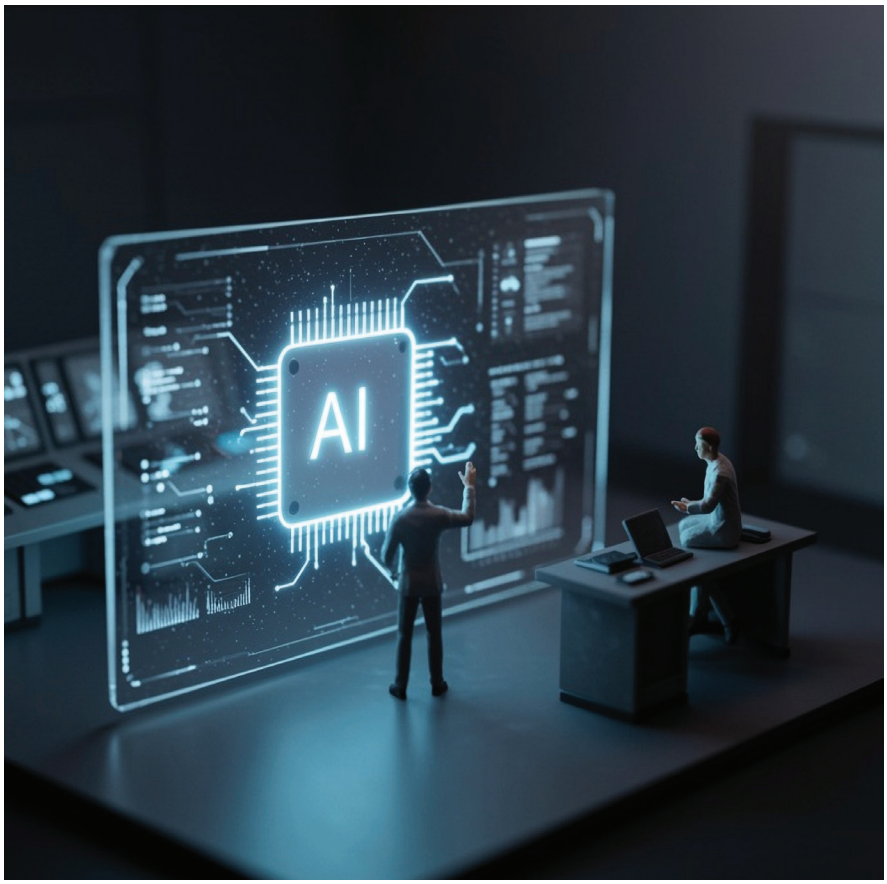
SNOWFLAKE has announced its intention to acquire Observe, a provider of AI-powered observability. This acquisition aims to enhance AI observability using open standards to support modern AI-driven enterprises.

According to Snowflake CEO, Sridhar Ramaswamy, reliability is no longer just an IT metric but an important factor for business operations.

By integrating Observe's capabilities, Snowflake aims to extend its AI Data Cloud, helping enterprises to manage vast telemetry data effectively.

Observe was created on the Snowflake platform, and their alliance aims to offer the following:

- Agentic AI for Enhanced Troubleshooting: Combined resources aim to allow companies to transition from traditional monitoring to proactive resolution strategies. The integration offers a unified context graph, improving the approach to troubleshooting.
- Open-Standard Architecture: By adopting standards like Apache Iceberg and OpenTelemetry, Snowflake and Observe aim to manage large data volumes efficiently, while applying analytics and AI uniformly.
- Efficient Economic Solutions: This collaboration addresses the high costs associated with observability data. It provides organisations a means to maintain telemetry data without economic trade-offs, enhancing both visibility and cost-effectiveness.



Jeremy Burton, CEO of Observe, emphasised the significance of this acquisition, noting its potential to enhance their observability solutions on an enterprise scale. The focus of AI has shifted, and the collaboration between Snowflake and Observe addresses these evolving challenges.

Sanjeev Mohan, Principal Analyst at SanjMo, reflected on the increasingly blurred lines between data and observability platforms. Snowflake's acquisition underlines this industry shift.

Once the acquisition is finalised, Snowflake plans to extend its IT operations management offerings in a market noted for recent growth by Gartner.

Reliability is no longer just an IT metric but an important factor for business operations. By integrating Observe's capabilities, Snowflake aims to extend its AI Data Cloud, helping enterprises to manage vast telemetry data effectively

TXP acquires Vigil to strengthen digital transformation services

TXP announces its acquisition of Vigil, an AWS specialist, to enhance its UK digital transformation offerings.

TXP has acquired Vigil, an AWS Select Tier Services Partner, as part of its strategy to develop its digital transformation business in the UK. This move aims to strengthen TXP's consulting, development, and resourcing solutions, particularly catering to its diversified clientele.

Vigil is recognised for its expertise in AWS-based cloud transformation, software engineering, and tech advisory services. These competencies complement TXP's existing cloud capabilities, seeking to enable an enhanced service delivery.

With a technology team of nearly 100 professionals primarily based in Portugal and Brazil, Vigil offers a broad selection of clients including ITV, Trainline, Convex, and DC Thomson Group. Their software engineering is positioned to extend TXP's nearshore and offshore offerings, and aims to support the company's strategy of delivering cost-effective yet quality-rich solutions.

John Antunes, CEO at TXP, remarked how Vigil's AWS proficiencies harmonise with TXP's Microsoft capabilities and add to TXP's technical capabilities and support client digital transformation efforts.

Phil Wright, CEO of Vigil, and his senior management aim to integrate with TXP's team and Aliter to drive ambitious growth plans. Phil Wright expressed enthusiasm about this collaborative venture, emphasising their shared focus on bespoke solutions and innovation.

This acquisition aligns with Aliter Capital's strategy to expand its presence in the UK digital transformation market. Aliter is focused on expanding TXP with further acquisitions that add relevant skills and capabilities, backed by organic growth.

Vigil is the fourth milestone in The Group's expansion, following the procurement of Gen modernisation specialist Metatech in May 2025.

A shift in ransomware tactics: Manufacturing faces new challenges

Manufacturing sectors see a shift in ransomware tactics as data theft rises. Defensive measures improve, yet pressure from adversaries persists.

SOPHOS has unveiled new insights from its State of Ransomware in Manufacturing and Production 2025 report. A significant highlight from the findings is the changing landscape of ransomware attacks on the manufacturing sector. While encryption rates have notably decreased, adversaries are choosing alternative tactics, such as data theft and extortion.

The report, based on a survey of 332 manufacturing organisations impacted by ransomware, exposes several concerning trends:

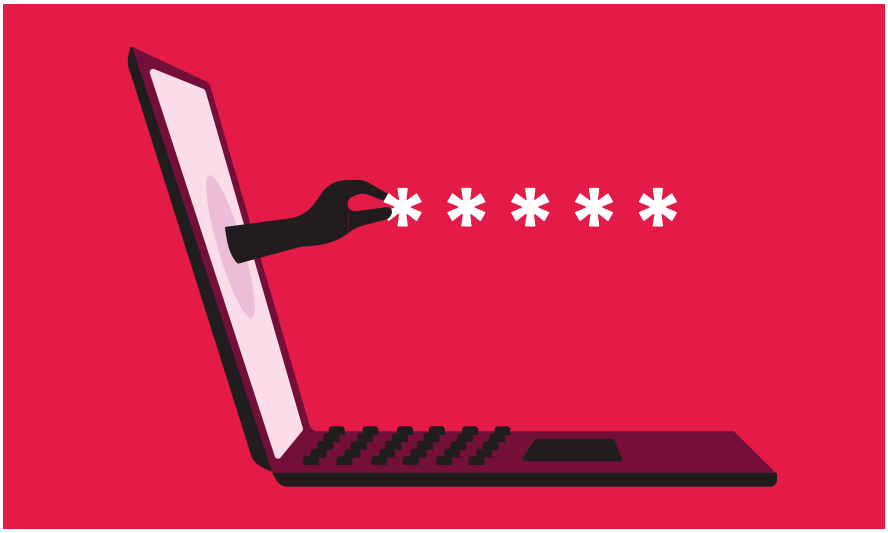
- Decline in Encryption: 40% of attacks resulted in data encryption, the lowest in five years, compared to 74% previously. However, extortion-only attacks, predicated on stolen data, rose to 10% from 3% in the prior year.
- Persistent Data Theft: Among manufacturers experiencing encryption, 39% also suffered data theft, marking a high incidence across surveyed sectors.
- Improved Deterrent Capabilities: An encouraging 50% of manufacturing entities thwarted attacks before encryption occurred, up from 24% last year.
- Skills and Protection Gaps: Lack of expertise and unrecognised security weaknesses contribute significantly to vulnerabilities, as identified by 42.5% and 41.6% of organisations respectively.
- Ransom Payments Remain High: Despite progress, 51% of impacted firms succumbed to paying the ransom, with a median payment of $1 million.
- Quicker Recoveries: Recovery costs have reduced, averaging $1.3 million, with 58% of organisations recovering fully within a week—up from 44%.
- Impact on Teams: Post-incident, 47% reported heightened stress within IT and security teams, while 44% faced increased leadership pressure.

Alexandra Rose, Director of Threat Research at Sophos Counter Threat Unit, emphasises the pressure the industry faces, highlighting the dependency on interconnected systems where even minor downtimes pose substantial supply chain risks.

Further investigations by Sophos X-Ops highlight notable ransomware activities from distinct threat groups like GOLD SAHARA, GOLD FEATHER, and GOLD ENCORE. These groups are increasingly employing double extortion tactics, both encrypting and stealing data, to hold organisations ransom with threats of data leaks.

Sophos recommends preventive measures to combat evolving cyber threats:

- Address Root Causes: Proactively resolve technical and operational flaws that adversaries often exploit.
- End-to-End Endpoint Protection: Every server and endpoint must have tailored anti-ransomware defences.
- Actionable Incident Response Plans: Regularly test and refine incident response strategies. Maintain consistent data backups to ease restoration and reduce downtime.
- Continuous Monitoring: Implement round-the-clock monitoring, potentially through a managed detection and response provider, strengthening overall threat detection and response.



Can AI help employees to upskill?

BY NADIR MERCHANT, GENERAL MANAGER, IT OPERATIONS SUITE, KASEYA

A RECENT MIT study suggested that the use of artificial intelligence (AI) may harm critical thinking. It was not the first study that came to that conclusion: A Microsoft poll of knowledge workers earlier this year also implied that GenAI usage may have a negative impact on thinking abilities. It argued that GenAI shifts the nature of critical thinking towards information verification, response integration and task stewardship, and observed that when users had higher confidence in GenAI, this appeared to be associated with less critical thinking.

While these studies make great headlines, the use of AI tools has, however, become an undeniable reality in everyday business. AI usage will only grow. And experience shows us that rather than making us less intelligent, AI can be a powerful tool in helping employees upskill. The right use of AI can make workers smarter, not less capable.

The study findings resonate because many users who are new to AI tools tend to hand tasks to AI without thinking. Asking ChatGPT or Microsoft Copilot to produce entire reports and presentations means previously time-consuming jobs can now be completed with minimal effort. This 'do it for me' mindset creates the illusion of efficiency, but it reduces the learning opportunity. And without human input, the results may look shiny but often turn out to be flawed.

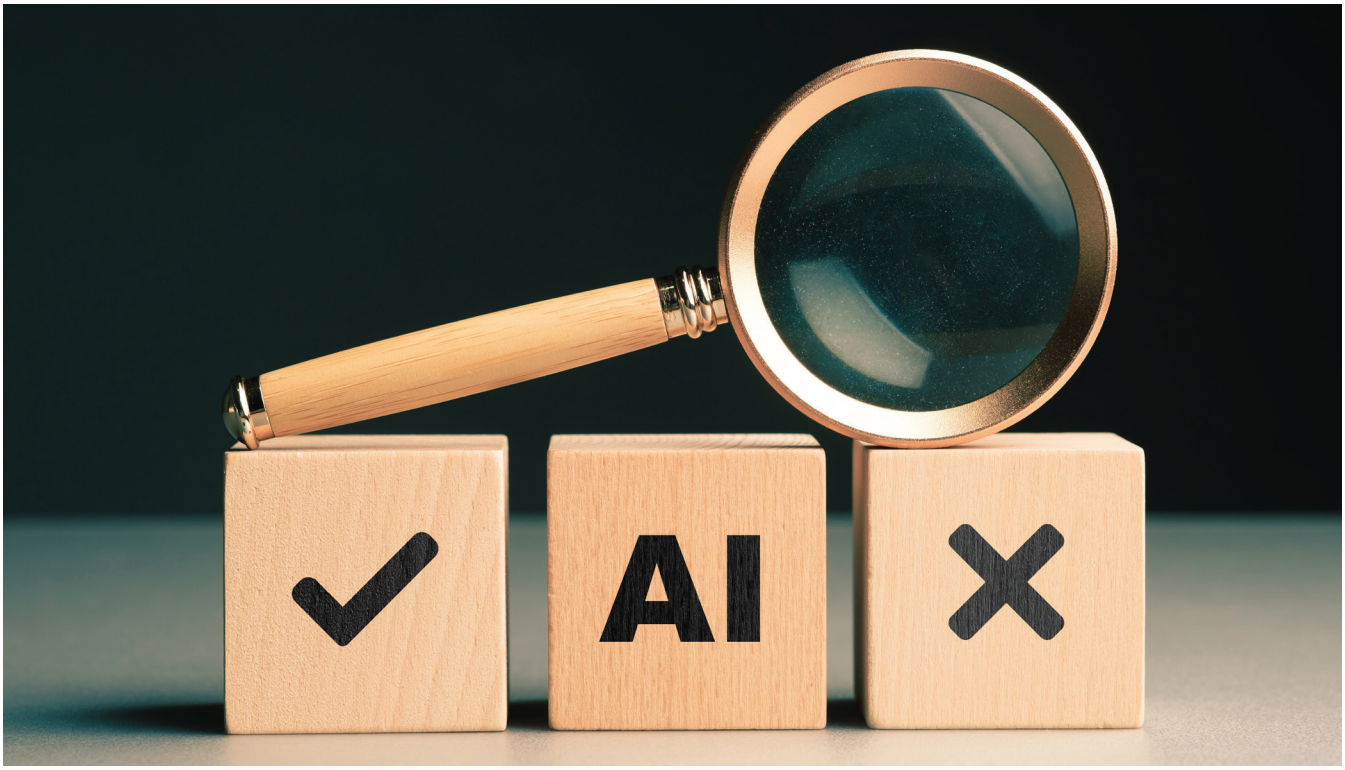
But, when we accuse AI of dumbing us down, perhaps we are blaming the wrong thing. AI isn't the problem. The way people use it is.

Stop using AI as a shortcut

The behaviour that can damage critical thinking is misusing AI as a shortcut to complete whole tasks – thereby avoiding work entirely. This over-reliance is a common problem. Take the example of writing a report. An employee might share bullet points, documents or a call recording with ChatGPT and tell it to create the full report from scratch. This cuts the time spent on the report from 8 hours to 3 minutes – and the employee's own input to zero, with a very likely impact on the quality of the report.

There is another, better way. Instead of asking AI to think for them, employees should think with the technology. Just like an assistant, an AI tool can provide support. It can help workers develop and augment their skills – not to mention do much of the legwork, but it still needs human oversight. A middle ground for producing the report would be to let AI collate, tidy up and structure information and draft an outline. The human's job then is to take over and edit, expand, verify and refine the draft.

When used in this way, the time spent on the report might drop from 8 hours to 2 hours rather than minutes. This is



still a considerable time saving, and it gives a better result. And with this more intelligent and effective way to use AI, learning improves, too.

AI is already a teacher

Many employees are already developing skills and absorbing knowledge through AI every day without realising it. Even in the most basic application of AI, where it essentially serves as a smarter search tool, the way workers use it has quietly shifted from "searching for information" to "interacting with a tutor". This is because AI doesn't only deliver the facts, but can also provide more detailed insights, examples, comparisons and step-by-step guidance, when asked. The technology is fantastic at researching, sifting through information and highlighting patterns, all of which help users digest information faster.

Increasingly, users are also harnessing AI tools to teach them new knowledge. Examples for this might be understanding product management frameworks or learning new programming languages. These are hybrid tasks where users don't just ask AI to do something for them but also learn through the interaction – for instance, by requesting practical scenarios or explanations at different levels of complexity. All of which helps them develop new skills at their own pace.

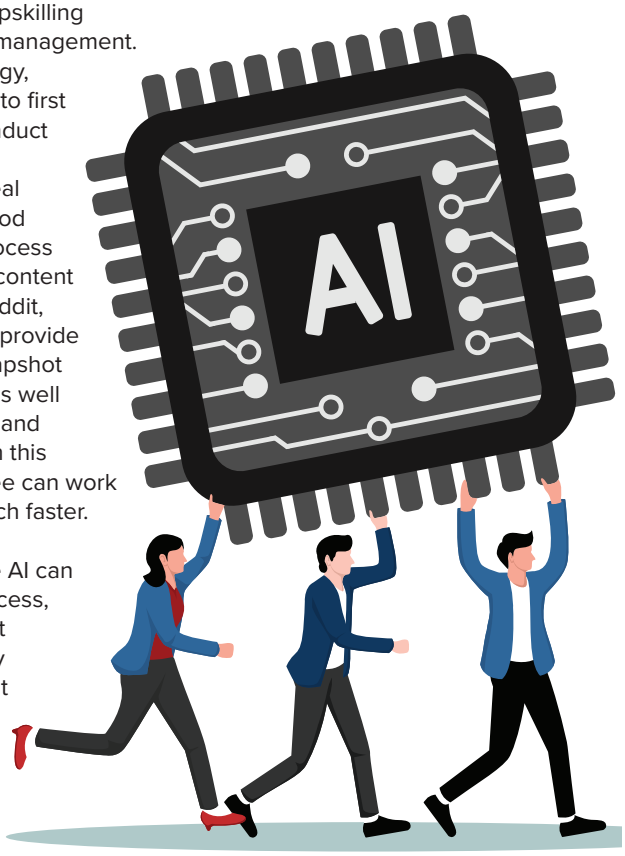
This shift is healthy, as long as organisations guide it. Indeed, when used well, AI could become one of the most powerful upskilling accelerators the workforce has ever had – helping employees learn faster, be better informed, think more broadly and ultimately, perform at a higher level.

AI can be transformative

Of course, there are limits to what AI can teach. Due to its nature, it is best for knowledge that can be acquired in self-directed study – such as how to build a survey questionnaire or structure a CV – and that don't require formal training or specialist qualifications. Because it can sort through facts fast and effectively summarises the most common expert answers from across the internet, it teaches best practices, helping even junior colleagues punch above their weight.

One good example for upskilling through AI is in product management. To determine their strategy, product managers need to first understand markets, conduct competitive analysis and gather sentiment from real users. AI is extremely good at this because it can process huge volumes of online content from sources such as Reddit, reviews and forums and provide an almost immediate snapshot of customer sentiment, as well as pinpointing strengths and weaknesses. Armed with this knowledge, the employee can work at a higher level and much faster.

On the other hand, while AI can support the learning process, it is less powerful when it comes to teaching highly advanced disciplines that require supervised practice and formal accreditation.



Another limitation is that AI delivers information but doesn't automatically test you. Many users don't realise that they can request quizzes, exercises or assessments to consolidate their learning.

Adoption isn't optional

In three years' time, nearly every organisation will use AI for employee skill development, whether they plan to or not. Trying to ban AI would be unrealistic. The most forward-thinking companies are already buying tools and encouraging AI-supported learning.

While currently, this mainly happens through general-purpose LLMs, in the future, we will see specialised AI learning tools, AI-powered courses and guided learning experiences, as well as more audio and video-based output formats.

However, AI will supplement, not replace traditional training – just like online learning didn't replace textbooks. People have different learning preferences and will expect a mix of materials, interactive learning and offline courses.

Additionally, while it's time to rethink how we teach skills, formal evaluation and accreditation still matter.

For those organisations wanting to embrace the trend now, the advice is to lead responsibly. Many of the day-to-day capability and productivity gains now happen inside AI tools, but AI usage needs guardrails. As well as providing company-approved, secure AI platforms, businesses should establish and enforce strong data protection and privacy guidelines. They should stipulate that AI tools need human oversight. Training is key, too, teaching employees how to use AI well, encouraging critical thinking and setting expectations around source verification and careful fact-checking instead of over-reliance on AI outputs.

Organisations should also foster a culture of healthy scepticism. AI can mislead when it relies on the wrong data. But its strength is that it lets users interrogate the information presented. Learners should always be encouraged to ask for evidence, cross-check and iterate.

Critical thinking isn't harmed by AI. It is harmed by unquestioning use. When embraced with the right mindset, it can make us smarter. Organisations that lean into AI for upskilling will build stronger workforces. Those that resist will fall behind.

As we take a moment to champion and celebrate the winners of the **2025 Channel Awards**, we recognise the visionaries who are shaping the future of the MSP ecosystem. These awards don't just honour excellence, they highlight the **innovations**, **projects**, and **leadership** that will define the next era of IT services. From AI-driven automation and intelligent cybersecurity to high-performance storage, cloud transformation, and forward-thinking service models, the winners are setting new benchmarks for efficiency, resilience, and growth. By celebrating these achievements, we shine a spotlight on the technologies and teams that empower **MSPs to deliver smarter, faster, and more strategic services**, building the foundation for a dynamic, future-ready channel.

PROJECT EXCELLENCE AWARDS

AWARD: Storage Project of the Year

WINNER: PURE STORAGE

RUNNERUP: ACRONIS

Pure Storage earned recognition for transforming how exabyte-scale scientific data is stored and accessed through its partnership with CERN openlab. By deploying DirectFlash technology, Pure Storage enables faster, denser, and more energy-efficient storage for the Large Hadron Collider, addressing the bottlenecks of traditional systems. This collaboration optimises high-performance computing and Grid workloads, ensuring researchers can capture, analyse, and share unprecedented volumes of data with speed and reliability. For MSPs and enterprise IT, the work demonstrates how cutting-edge flash storage can scale to extreme demands while improving operational efficiency, setting a benchmark for future-ready, sustainable data infrastructure across research and high-performance environments.

AWARD: Cyber Resilience Project of the Year

WINNER: VIZST TECHNOLOGY

RUNNERUP: PERFORMANTA

Vizst Technology's project demonstrates how strategic IT modernisation can enhance cyber resilience in retail. Over 45 days, the team implemented a cloud-first, SASE-based architecture across 100 Crew Clothing sites, consolidating fragmented legacy systems while maintaining zero downtime. Centralised visibility, integrated security, and cloud migration improved threat detection and reduced vulnerabilities, shifting IT focus from reactive support to strategic innovation.

By ensuring operational continuity, strengthening security controls, and future-proofing infrastructure, the initiative shows how agile, business-aligned transformation can protect critical systems, enable secure growth, and serve as a practical model for cyber-resilient digital transformation.

AWARD: Cloud Transformation Project of the Year

WINNER: TMB SYSTEMS LIMITED

RUNNERUP: BIZACUITY SOLUTIONS PVT. LTD

TMB's project demonstrates how strategic cloud identity management can modernise complex, multi-site operations. By migrating 40 hotels to Microsoft Entra ID, TMB centralised access control, deployed multi-factor authentication, and integrated Microsoft 365 services, removing legacy servers and improving operational efficiency. A phased rollout ensured continuity across dispersed sites, while SSO and cross-tenant collaboration enhanced productivity. Beyond performance improvements, the initiative reduced energy consumption, standardised licensing, and strengthened security. By aligning technical delivery with business priorities, TMB showed how targeted cloud transformation can future-proof infrastructure, support sustainability, and deliver measurable efficiency and resilience benefits.

AWARD: Communications & Networking Project of the Year

WINNER: HYVE MANAGED HOSTING

RUNNERUP: TMB SYSTEMS LIMITED

Hyve Managed Hosting's partnership with Digital Realty demonstrates how strategic alliances can expand global capacity and strengthen network resilience. By leveraging Digital Realty's ServiceFabric® interconnection and deploying at the LON2 data centre, Hyve enhances ultra-low latency connectivity, disaster recovery, and operational reliability for enterprise clients. The collaboration provides scalable access to over 300 data centres worldwide while aligning with sustainability goals through renewable energy. This initiative highlights how combining high-performance infrastructure, interconnectivity, and strategic vendor partnerships can enable enterprise-grade, resilient networking solutions, support global expansion, and deliver measurable benefits for customers across multiple sectors.

AWARD: Digital Transformation Project of the Year

WINNER: SCHNEIDER ELECTRIC AND ADVANCED POWER TECHNOLOGY (APT)

RUNNERUP: VIZST TECHNOLOGY

Schneider Electric and Advanced Power Technology partnered with Queen Mary University of London to modernise its research data centre, combining resilience, scalability and sustainability. EcoStruxure solutions including InRow cooling, DCIM monitoring and thermal containment improved uptime, enabled high performance workloads and redirected waste heat to the campus heating network, cutting emissions and costs. Predictive monitoring and automated alerts reduce downtime and manual intervention, enhancing operational efficiency. This project demonstrates how intelligent, energy efficient infrastructure can advance research while supporting sustainability, setting a new benchmark for modern, high performance data centres.

AWARD: Cybersecurity Project of the Year

WINNER: INTERGENCE

RUNNERUP: ADM

Intergence partnered with Tendring District Council to enhance its cybersecurity posture through the deployment of a modern, AI-driven SIEM. By automating log correlation and threat detection, the project shifted the council from reactive monitoring to proactive, intelligence-led security. High-fidelity alerts, three-stage containment, and continuous machine learning reduced analyst workload and accelerated response times.

This approach strengthened resilience across critical services while freeing internal teams to focus on strategic initiatives. The project demonstrates how predictive and automated security solutions can deliver practical efficiency, improved protection, and actionable insights at scale for public sector organisations.

AWARD: AI & Automation Project of the Year

WINNER: LAPSAFE

RUNNERUP: THRIVE

LapSafe®'s AI Smart Locker transforms device management by automating loans, returns, swaps, and servicing, while AI predicts faults, monitors usage, and flags maintenance requirements. Fully integrated with the ONARKEN® platform and smart power management, it reduces administrative burdens, accelerates turnaround times, and improves visibility across all assets. What makes this solution particularly significant is how it shifts the role of a locker from a passive storage unit to a proactive, data-driven service platform. By turning routine device management into an intelligent, automated process, LapSafe® demonstrates how MSPs can gain operational efficiency, minimise errors, and deliver faster, more reliable service.

TECHNOLOGY INNOVATION AWARDS

AWARD: Backup & DR Innovation of the Year

WINNER: EXAGRID

RUNNERUP: BRIDGEWORKS

ExaGrid's Tiered Backup Storage was recognised for Backup & DR Innovation of the Year for its distinctive approach to data protection. Its high-speed Landing Zone, scale-out architecture, and secure, non-network-facing Repository Tier deliver fast backups and restores while reducing storage requirements. Integration with leading backup applications, support for advanced encryption, and robust ransomware and disaster recovery capabilities set it apart from traditional solutions. Recent enhancements, including Rubrik and MongoDB support and improved governance features, demonstrate how ExaGrid combines performance, security, and operational flexibility. This offers MSPs a practical, innovative solution to evolving backup and recovery challenges.

AWARD: Storage Software/Management Innovation of the Year

WINNER: STORMAGIC

RUNNERUP: OPEN-E

StorMagic SvHCI earned recognition for delivering hyperconverged infrastructure built for the enterprise edge, remote offices, and SMBs. Combining virtualised storage, networking, and compute in just two nodes, it provides high availability, rapid VM failover, and simplified management without onsite IT staff. Integration with existing VMware environments, lightweight deployment, and 24/7 support make it both cost-efficient and operationally resilient. For MSPs, SvHCI demonstrates how purpose-built, edge-optimised HCI can reduce hardware dependency, streamline operations, and lower total cost of ownership while maintaining enterprise-grade reliability, setting a new benchmark for modern, scalable infrastructure at distributed sites.

AWARD: Cyber Resilience Innovation of the Year

WINNER: OPENGEAR

RUNNERUP: INFINIDAT

Opengear's CM8100-10G-5G demonstrates how integrating 5G into console management enhances cyber resilience and operational continuity. By combining high-speed 10GbE uplinks with failover-ready 5G connectivity, the solution ensures uninterrupted access to critical infrastructure while simplifying network management for up to 48 devices. Scalable, adaptable, and optimised for AI, cloud, and IoT environments, it provides visibility, control, and automatic failover during disruptions. This development shows how forward-looking network management can safeguard complex IT estates, maintain business continuity, and reduce operational overhead, providing organisations with a resilient platform to meet evolving technological demands.

AWARD: Storage Hardware Innovation of the Year

WINNER: EXAGRID

RUNNERUP: OBJECT FIRST

ExaGrid's Tiered Backup Storage was recognised for its combination of performance, scalability, and security. Its unique disk-cache Landing Zone accelerates backups and restores, while the Repository Tier reduces long-term storage costs and supports ransomware recovery.

The scale-out architecture allows up to 6PB of full backups in a single system. Integration with Rubrik, MongoDB Ops Manager, and major backup applications, alongside advanced encryption, dedicated networks, and secure management, demonstrates how ExaGrid delivers a flexible, resilient, and efficient hardware platform that meets the evolving needs of MSPs and enterprise backup environments.

AWARD: Cybersecurity Innovation of the Year

WINNER: HORNETSECURITY

RUNNERUP: THREATLOCKER

Hornetsecurity's AI Cyber Assistant enhances Microsoft 365 protection by integrating AI-driven threat detection, real-time monitoring, and user education in a single platform.

Automating email report analysis and extending security into Teams helps reduce SOC workload while supporting stronger end-user awareness. By applying machine learning, computer vision, and large language model technology, the solution enables MSPs and IT teams to address evolving threats more efficiently. This combination of automation, visibility, and operational support demonstrates how intelligent tools can improve security, compliance, and resilience within Microsoft 365 environments, providing practical benefits for organisations and their IT teams.

AWARD: Cloud Services Platform of the Year

WINNER: VEEAM

RUNNERUP: AIR IT GROUP

Veeam Data Cloud Vault offers MSPs a practical, secure approach to cloud backup by combining enterprise-grade security, Zero Trust principles, and fully managed, predictable storage. In a market where ransomware, compliance requirements, and rising cloud costs create real operational pressures, it gives MSPs the tools to protect client environments reliably and at scale. By simplifying a traditionally complex area of IT management, Veeam Data Cloud Vault allows MSPs to focus on delivering consistent, resilient services while maintaining full control and oversight. This illustrates how thoughtful cloud innovation can support both operational efficiency and client trust.

AWARD: AI or ML Innovation of the Year

WINNER: KASEYA

RUNNERUP: THRIVE

Kaseya 365 Ops gained recognition for showing how AI can fundamentally reshape IT management for MSPs, not just by automating tasks, but by rethinking the entire workflow. By unifying PSA, documentation, billing, and reporting into a single intelligent platform, it eliminates tool sprawl and brings real-time, actionable insights directly to technicians. This allows IT teams to prioritise high-value work instead of spending time on repetitive, manual processes. In an industry where efficiency, visibility, and scalability are paramount, Kaseya 365 Ops stands out for turning AI from a buzzword into a practical, transformative tool for service delivery.

AWARD: Remote Monitoring & Management (RMM/PSA) Tool of the Year

WINNER: N-ABLE

RUNNERUP: NINJAONE

N-able is transforming IT and security operations by integrating Vulnerability Management directly into its UEM platforms, N-central and N-sight. The built-in capability allows IT teams to continuously identify and remediate OS and application vulnerabilities from a single interface, streamlining workflows and improving cyber resilience. By automating patching and remediation, N-able helps MSPs and IT professionals manage modern threats more efficiently. With continuous scanning, detailed risk insights, and plans to extend coverage to network and cloud environments, the company shows how intelligence-driven tools can empower IT teams to protect organisations proactively while reducing operational burden and risk.

AWARD: Data Management & Analytics Innovation of the Year

WINNER: ZOHO

RUNNERUP: CITIC TELECOM CPC

Zoho Analytics 6.0 integrates AI-powered self-service BI capabilities, combining AutoML, predictive insights, and natural language querying through Zia. The platform enables users to diagnose performance changes, uncover trends, and generate reports automatically, while also supporting custom ML model building and third-party BI integration. Enhanced visualisations improve clarity and actionable insight, giving organisations the ability to make data-driven decisions more efficiently. By embedding AI into analytics, Zoho demonstrates how flexible and scalable solutions can support smarter interpretation and utilisation of data, helping businesses act confidently across diverse operational environments.

MSP & RESELLER AWARDS

AWARD: Specialist MSP of the Year

WINNER: TMB SYSTEMS LIMITED

RUNNERUP: ASSURED DATA PROTECTION

TMB Systems stands out as a specialist MSP by delivering IT and cybersecurity services tailored specifically to the hospitality sector. Its co-managed model combines client control with 24/7 support from dedicated account managers, service teams, and a round-the-clock service desk, while third-party fault management reduces downtime and eases internal workloads. TMB's services cover critical hotel systems, including property management, telephony, CCTV, access control, and guest Wi-Fi, all aligned with operational and brand standards. SOC 2 compliance and strategic projects, such as cloud transformation for Valor Hospitality, highlight both security and scalability. TMB exemplifies how sector-focused MSPs can deliver reliable, compliant, and globally consistent IT support.

AWARD: MSSP (Managed Security Services Provider) of the Year

WINNER: LITTLEFISH

RUNNERUP: AIR IT GROUP

Littlefish combines people-centred cybersecurity with AI-driven innovation to deliver reliable protection across sectors from healthcare to government. Its CREST-certified Security Operations Centre uses bespoke tools, including DeepDefend, to automate alerts, reduce analyst workload, and proactively detect vulnerabilities, while the Critical Hour framework tailors incident response to each client's needs. Rapid growth of 360 percent in under four years reflects the effectiveness of pairing technical excellence with user-focused service. Through the Littlefish Academy and integration of intelligence from industry and government sources, the company demonstrates how a human-led, innovation-focused MSP can deliver adaptive, resilient security at scale.

AWARD: Emerging MSP of the Year

WINNER: SOTS – SUPPORT ON THE SPOT LIMITED

RUNNERUP: DUNEDIN IT

SOTS – Support on the Spot Limited delivers security-focused managed services covering IT support, cybersecurity, cloud infrastructure, VoIP, software licensing, and device management. Their coordinated approach helps minimise downtime and maintain client trust while addressing operational and strategic IT needs. SOTS enhances client agility, retains a high level of customer satisfaction, and supports digital initiatives across IT, marketing, and design. By combining technical expertise with responsive service delivery, SOTS provides a reliable foundation for end-to-end device management and demonstrates how emerging MSPs can support growth and resilience in evolving IT environments.

AWARD: MSP of the Year (UK)

WINNER: ADVANIA

RUNNERUP: VERSION 1

Advania UK earned MSP of the Year by showing that growth and a people-centred approach can coexist at scale. Its service culture, built on technical expertise and long-term trust, underpins a portfolio spanning cloud, cybersecurity, unified communications, and digital transformation.

With a long-standing Microsoft partnership and Azure Expert MSP status, Advania consistently delivers outcomes that matter to clients, reflected in high satisfaction scores. Its success highlights how genuine partnership, rather than transactional service, can define managed services in a rapidly evolving market.

AWARD: IT Reseller/VAR of the Year

WINNER: VIZST TECHNOLOGY

RUNNERUP: SUMILLION LIMITED

Vizst Technology demonstrates how a partner led approach can combine technical innovation with strategic business impact. By launching Vizion by Vizst, a fully managed intelligence led solution integrating Gigamon, Vectra, and Forescout, the company simplified complex technologies while generating significant pipeline growth. Their work on Crew Clothing's rapid SASE and cloud transformation further illustrates their ability to deliver scalable, secure, and business aligned outcomes. Complemented by investment in people, operational maturity, and thought leadership initiatives, Vizst shows how a VAR can drive market influence, strengthen vendor and customer partnerships, and transform IT from a support function into a growth enabler.

AWARD: MSP of the Year (EMEA)

WINNER: TMB SYSTEMS

RUNNERUP: EPX TECHNICAL SERVICES

TMB Systems' hospitality-focused approach highlights how sector-specific expertise can set an MSP apart. Its co-managed model, combined with support for telephony, access control, and guest Wi-Fi, ensures continuity and operational relevance across single sites and multi-country operations. A 24/7 engineering desk, dedicated account managers, and third-party fault management provide consistent, reliable service. Projects such as modernising Valor Hospitality's IT infrastructure demonstrate scalability, enhanced security, and improved collaboration. By aligning technical delivery with operational priorities, TMB illustrates how a specialist MSP can drive measurable impact, reliability, and resilience across a complex EMEA client base.

VENDOR & DISTRIBUTOR CHANNEL AWARDS

AWARD: Vendor Channel Programme of the Year

WINNER: LENOVO

RUNNERUP: CHECK POINT SOFTWARE

Lenovo has been recognised for reshaping how MSPs engage with a global technology partner, creating a program that simplifies access to training, certifications, marketing resources, and flexible solutions. Launched in 2024, the initiative provides a unified, incentive-driven pathway across Lenovo's full portfolio of devices, infrastructure, and services. By removing traditional barriers such as tiering or revenue thresholds, Lenovo 360 enables MSPs of all sizes to participate fully. Early success in EMEA, the Americas, and Asia-Pacific demonstrates its scalability and partner appeal, showing how a vendor-led program can streamline operations, drive recurring revenue, and support differentiated, outcome-focused services at scale.

AWARD: Vendor Marketing/Enablement Initiative of the Year

WINNER: SOPHOS

RUNNERUP: EXAGRID

Sophos' MSP Community Days exemplify how vendor-led initiatives can strengthen partner engagement and drive practical business outcomes. Launched across the UK, Benelux, and Central Europe, the program combined expert-led briefings, interactive exercises, and peer learning to translate complex cybersecurity concepts, such as Managed Detection and Response, into actionable strategies. Marketing and business masterclasses equipped MSPs with tools to enhance go-to-market capabilities, while networking sessions fostered collaboration and community. By blending education, hands-on guidance, and peer interaction, the initiative demonstrated a structured approach to empowering partners, deepening relationships, and supporting sustainable growth in the MSP ecosystem.

AWARD: Cybersecurity Vendor of the Year

WINNER: OPENTEXT CYBERSECURITY

RUNNERUP: KASEYA

OpenText Cybersecurity supports MSPs in delivering enterprise-grade protection at scale through its enhanced Secure Cloud platform. By streamlining service delivery, automating workflows, and providing integrated reporting, the platform enables partners to operate efficiently and respond to evolving threats. OpenText also invests in partner enablement with targeted training, go-to-market support, and threat intelligence, strengthening skills and engagement across its ecosystem. This approach illustrates how a purpose-built, end-to-end cybersecurity platform can help MSPs scale confidently, maintain operational efficiency, and provide trusted, comprehensive protection to customers across diverse environments.

AWARD: Cyber Resilience Vendor of the Year

WINNER: CYBERGLOBAL

RUNNERUP: VEEAM

CyberGlobal exemplifies how a partner-focused approach can advance cyber resilience across the MSP ecosystem. Through its MSP Partner Program, the company enables providers to deliver enterprise-grade services, including SOC, penetration testing, and compliance audits. White-label solutions, training, and dedicated support empower partners to expand offerings, strengthen client security, and meet regulatory requirements efficiently. Real-world engagements, such as hardening a Romanian software firm and developing 1,600 threat detection rules with Anvilogic, demonstrate measurable improvements in threat detection, remediation, and operational resilience, positioning CyberGlobal as a trusted enabler of secure, scalable cybersecurity solutions.

AWARD: Storage Vendor of the Year

WINNER: EXAGRID

RUNNERUP: INFINIDAT

ExaGrid was recognised for its Tiered Backup Storage platform, which separates high-speed backups and restores through a front-end Landing Zone from long-term retention in a non-network-facing Repository Tier. Its scale-out architecture maintains performance as data grows, while integration with over 25 backup applications supports diverse environments. Additional features, including Rubrik and MongoDB support, advanced encryption, dedicated managed networks, and disaster recovery capabilities, provide operational flexibility and security. These practical design choices demonstrate why ExaGrid's approach was considered notable in addressing the evolving storage and data protection needs of MSPs.

AWARD: Distributor of the Year

WINNER: ARROW ECS

RUNNERUP: GAMMA

Arrow ECS UK's MSP Team supports MSPs, MSSPs, and CSPs with specialist expertise and value-added services. Using the ArrowSphere cloud platform and a portfolio of over 100 vendors, the team simplifies cloud adoption, management, and recurring revenue generation. The Cloud Innovation programme aligns solutions with partner growth objectives, while Arrow Smart Finance provides flexible options to accelerate deals and improve profitability. End-to-end support includes consultation, installation, testing, auditing, and 24/7 managed services for cloud backup, networking, and security. With marketing and go-to-market support, Arrow ECS UK enables partners to scale operations, strengthen client relationships, and achieve measurable business outcomes.

AWARD: Cloud / Value-Added Distributor of the Year

WINNER: INFINIGATE CLOUD

RUNNERUP: EXCLUSIVE NETWORKS

Infinigate Cloud demonstrates how a distributor can drive measurable growth and enablement across the MSP ecosystem. By expanding the CORE Marketplace, onboarding leading security vendors, and providing integrated cloud solutions, the company simplifies service provisioning and reduces operational complexity. Its partner enablement programmes, EDGE for technical training and certification, GROW for marketing support, and PRO for professional services, have strengthened partner capabilities, increased margins, and supported revenue growth. With scalable platform enhancements, strong partner acquisition, and demonstrable business impact, Infinigate Cloud shows how a cloud-focused distributor can empower MSPs, integrate security and cloud services, and accelerate channel success.

AWARD: Marketplace Channel of the Year

WINNER: PAX8

RUNNERUP: ARROW ECS

Pax8 stands out this year for advancing what a modern technology marketplace can deliver to MSPs and their customers. Its recent developments, including tools that reveal gaps in a partner's technology stack and provide streamlined customer storefronts, reflect a clear push toward more efficient, intelligence driven service models.

With strong engagement across the UK and a growing global presence, Pax8 has helped MSPs respond to rapid changes in the market, particularly around artificial intelligence, security and cloud optimisation. These innovations point to a broader industry shift toward marketplaces that inform, guide and support the next stage of business growth.

PEOPLE, COMPANY & CULTURE AWARDS

AWARD: Technical or Service Excellence Team of the Year

WINNER: REJUVENATE IT

RUNNERUP: EXAGRID

Rejuvenate IT was recognised for combining technical expertise with a client-first ethos, delivering tailored solutions that meet the evolving needs of its customers. Supporting over 180 businesses across Dorset, Hampshire, and beyond, the team provides proactive, 24/7 IT support that reduces downtime, streamlines operations, and builds long-term client trust. ISO-certified and Cyber Essentials accredited, Rejuvenate IT pairs enterprise-level technology with a personal touch, ensuring fast, reliable, and jargon-free service. The team illustrates how a strong service culture drives client satisfaction, loyalty, and operational resilience, showing that consistent, human-centred support is as vital to success as the technology itself.

AWARD: DEI/ESG Programme of the Year

WINNER: NEBULA GLOBAL SERVICES

RUNNERUP: THRIVE

Nebula integrates ESG into core operations while supporting its partner ecosystem. Initiatives such as NebZero track carbon footprints and promote carbon-neutral events, reducing emissions and encouraging responsible consumption. Nebula also drives social impact through volunteer programs, community engagement, and local skills development. Through the launch of its Sustainable Business Report, engineer carbon footprint tracking, and the "ESG Unwrapped" insight platform, Nebula strengthens sustainability across the channel. By embedding environmental and social responsibility into daily practices, Nebula enables MSP partners to adopt greener operations while delivering measurable community and environmental outcomes.

AWARD: Channel Leader of the Year

WINNER: CHRIS WHITLEY – CHECK POINT SOFTWARE

RUNNERUP: JASON KEMSLEY - UPTIME GLOBAL

Chris Whitley exemplifies how strategic collaboration can strengthen the EMEA channel ecosystem. Known for his integrity, fairness, and customer-first approach, he aligns vendors, distributors, and partners around shared goals while ensuring decisions deliver long-term value. By orchestrating complex multi-party engagements and integrating partners into sales, marketing, and business operations, Chris enhances partner enablement, expands market reach, and drives sustainable growth. His leadership prioritises transparency and trust over short-term gains, setting a benchmark for ecosystem collaboration and demonstrating how principled, strategic channel management can create measurable business impact across diverse markets.

AWARD: Channel Company of the Year

WINNER: SOPHOS

RUNNERUP: GAMMA

Sophos has developed a channel-focused approach that helps MSPs deliver cybersecurity across on-premises, private, and public cloud environments. Supporting more than 440,000 organisations in over 150 countries, it enables partners to provide managed or self-managed services efficiently, addressing evolving threats while improving operational efficiency and controlling costs.

Integrated, adaptive solutions give service providers the tools to expand offerings, grow revenue, and deliver consistent protection. By combining scalability, flexibility, and effectiveness, Sophos demonstrates a practical model for helping MSPs navigate the increasing complexity of today's cybersecurity landscape.

MSP Channel Insights Roadshow:
Manchester Highlights a Thriving MSP Community

THE MSP CHANNEL INSIGHTS ROADSHOW returned to Manchester at the Hyatt Regency, bringing together MSP leaders, cybersecurity experts, and channel partners for a day that sparked insight, collaboration, and practical takeaways.

THE EVENT was expertly moderated by Alex Wood (Alex Wood Presents), guiding discussions and panels throughout the day. Manchester's growing reputation as a digital and tech hub made it the perfect setting, with attendees leaving inspired by the insights and strategies shared across a packed agenda.

The day opened with a Fireside Chat, Scaling Smart – A Candid Conversation with a High-Growth MSP, where Alex Heslip of Novem shared the journey of growing a business in a fast-moving, competitive market. Alex spoke candidly about navigating growth milestones, overcoming operational challenges, and adapting strategies to meet the evolving needs of clients. The conversation was refreshingly practical, filled with real-world examples and lessons learned that demonstrated how resilience and thoughtful planning can support sustainable growth.

The first panel, Cybersecurity & Resilience – Navigating Threats in an AI-Enhanced World, brought together David Clarke (The TrustBridge), Matt Fooks (VCG Technology Services), and Tom Heyes (Airwalk Reply) to unpack the challenges of a volatile cyber landscape. The discussion explored how AI is reshaping both defensive and offensive strategies, while offering practical insights on monetising security services, maintaining operational resilience, and staying compliant amid increasingly sophisticated threats. Micro insight sessions from NinjaOne, ThreatLocker, and The TrustBridge expanded on these themes, keeping ideas flowing and sparking lively discussion ahead of networking.

In the Smarter Sales & Marketing – Winning in a Crowded MSP Landscape panel, Graham Stead (Growth Habits), Edd Dale (Illuminate Learning), Joe Burns (Reformed IT), Stephen Grey (Westcoast Cloud), and Stephen Hobson (Apex Computing) shared practical strategies for differentiating MSPs in a competitive market. The conversation highlighted how data, AI, and vertical specialisation

can help partners win high-value clients and build repeatable, profitable growth. This flowed into the Strategic Insight Roundtable Sessions, where delegates rotated through sponsor-led small group discussions, exchanging ideas and exploring solutions that matter most to their businesses.

The day also featured a Compliance & Risk breakout hosted by The TrustBridge, which highlighted the fine line between operational responsibility and client risk ownership. Speakers emphasised that while MSPs manage systems, ultimate responsibility rests with clients, and clarity in contracts is essential. Delegates explored practical ways to strengthen compliance, from readiness assessments to thoughtful supply chain engagement, leaving with actionable insights on governance, documentation, and building scalable, risk-aware services.

The Sales breakout session hosted by Graham Stead of Growth Habits offered a grounded look at what it really takes to build and scale sales, whether MSPs already had a sales team or were still founder-led. The session focused on habits, structure, and coaching as the drivers of sustainable performance. The session explored common pitfalls such as hybrid role drift and the risks of hiring on instinct rather than evidence. A strong emphasis was placed on structured recruitment and 90-day onboarding, replacing the familiar "here's a laptop, go sell" model with defined milestones that surface success early. Commission design sparked lively discussion, particularly around simple, transparent, MRR-focused plans, supported by meaningful KPIs, realistic ramp times, and a long-term view of ROI in recurring revenue businesses.

The discussion focused on the importance of fostering a strong workplace culture to retain talented staff. Speakers explored ways to support individual needs while learning how to build agile, diverse workplaces where employees feel valued and empowered

Panel 3, People, Culture, Recruitment & DEI – The New Competitive Edge for MSPs, featured Hayley Carter (ESSENTIA), Natalie Hailey (Academia the Technology Group), Tom Marwood (Westcoast Cloud), and Zoe Chatley (The Channel Recruiter). The discussion reinforced that talent retention, company culture, and inclusion are strategic business imperatives, not just HR concerns. The discussion focused on the importance of fostering a strong workplace culture to retain talented staff. Speakers explored ways to support individual needs while learning how to build agile, diverse workplaces where employees feel valued and empowered. Speakers concluded that retention and workplace satisfaction goes beyond pay and includes recognition, career development, and a truly supportive culture.

The final panel, M&A, Investment & Growth Strategy – Building a Business That Scales or Sells, brought together Alex Heslip, Ken Roulston (Ex2 Consultancy), and Wernher Pikali (AION Succession Partners) to explore the challenges of MSP acquisitions. Through real-world examples, attendees saw how culture and people can make or break a deal. Clear succession planning, careful integration, and preserving continuity after a sale were shown to protect teams and create lasting value, highlighting the critical role of alignment, communication, and strategy in scaling or selling a business.

Overall, the MSP Channel Insights Manchester Roadshow left a strong impression. Attendees actively contributed to discussions that showcased the energy, expertise, and vibrancy of the MSP community. The event explored new approaches to business growth, addressed pressing challenges, and shared innovative ideas across cybersecurity, sales, people strategy, and M&A. The atmosphere reflected the dedication of all involved, from speakers and breakout hosts to sponsors who provided fresh perspectives.

A sincere thank you goes to the sponsors, delegates, and attendees who made the day so engaging and inspiring. The Roadshow reinforced why being part of this community is so valuable and left everyone looking forward to the next opportunity to connect, learn, and be inspired.

Small businesses at risk: How MSPs can navigate the AI-driven cybersecurity landscape

In an exclusive interview, Dor Eisner, Co-Founder and CEO of Guardz, reveals key insights into the cybersecurity landscape and the pressures shaping today's MSP environment.

SMALL and medium-sized businesses (SMBs) have long been considered attractive targets for cybercriminals, but the threat landscape is evolving faster than ever. Guardz's latest Cybersecurity SMB Report reveals that while awareness of cybersecurity risks is high among SMBs, preparedness remains critically low. In addition to insights from the Cybersecurity SMB Report, Dor Eisner, Co-Founder and CEO of Guardz, shares how artificial intelligence (AI) is accelerating attacks, placing SMBs at even greater risk, and why Managed Service Providers must adapt strategically to meet this growing demand.

The Rising Threat Landscape for SMBs

According to the Guardz report, almost 50% of SMBs have already experienced a cyber incident, yet only 34% have a formal incident response plan in place. This gap between awareness and readiness is alarming. SMBs recognise that the stakes are high, with 61% believing cybersecurity risks will increase in 2026, but many lack the operational structure, expertise, or resources to respond effectively.

AI is a game-changer in this context. Attackers now leverage large language models (LLMs), like ChatGPT, to automate account compromises, spear-phishing, and other attacks at scale. This "machine-speed" execution enables cybercriminals to target SMBs more efficiently, and many SMBs underestimate how quickly these attacks can disrupt operations. The smallest businesses, often lacking dedicated security teams, are the most vulnerable, making them prime targets in the evolving threat landscape.

Guardz's research finds that the financial impact of a single incident can reach seven figures, with recovery cycles extending for months. For many SMBs, human error remains the top vulnerability: 45% identified employee mistakes as the main cause of compromise. Combined with outdated technologies and unapproved third-party applications, SMBs operate in a fragmented security environment that leaves them exposed.

Why MSPs Are at a Critical Juncture

For MSPs, these findings present both a challenge and an opportunity. The report highlights that 52% of SMBs would seek assistance from an MSP due to fear of attack, signalling a rising market demand for professional, consolidated cybersecurity services. However, many MSPs are not yet fully equipped to meet this demand.

Eisner stresses that identity is now the new security perimeter. Traditional security approaches based on isolated detection for endpoints, email, or networks are no longer sufficient in an era where attackers exploit cloud identities, session tokens, and misconfigured access paths. MSPs must adopt identity-centric security models, correlating signals across attack vectors, mapping them to individual users, and communicating risk in measurable, client-specific terms.

This shift is particularly relevant for SMBs that rely on cloud services and distributed teams. Workspace security is evolving to incorporate real-time, device-centric context checks, and SMBs must ensure strong identity governance to maintain trust across their operations and supply chains.

The Case for Consolidated Platforms and Data-Led Automation

The report also emphasises the need for consolidated, affordable security platforms. Many SMBs attempt to piece together disparate point solutions, which are often complex, expensive, and difficult to integrate. This fragmentation increases operational burden and limits the effectiveness of monitoring, detection, and response efforts.

Automation is another critical factor, but it cannot succeed without a strong foundation of high-quality, correlated data. MSPs must implement proper controls and normalise security data to leverage AI for detection and response. Without unified infrastructure, automation remains partial, and the risk of missed threats grows. Unified platforms reduce operational costs for MSPs while strengthening the security posture of SMB clients, making comprehensive protection both feasible and sustainable.

Learning from Real Incidents

One of the most actionable insights from the Guardz report is the impact of formal incident response planning. Among SMBs that had a plan, 80% were able to avoid major damage. This highlights a clear path forward for MSPs: by guiding SMB clients in implementing structured, repeatable response processes, MSPs not only reduce risk but also establish trust and long-term value.

Yet, the report reveals a stark reality. While awareness of threats is high, SMBs' ability to manage them is limited. Less than half conduct regular security assessments, penetration testing, or cloud application security reviews. Email filtering, firewalls, and awareness training are more common, but even these foundational tools are often inconsistently applied. The result is a wide operational gap between potential and actual security readiness.

Future Threats: Identity and Data Exfiltration

Looking ahead to 2026, Eisner predicts that identity-focused attacks and AI-driven data exfiltration will dominate the threat landscape. Adversaries are expected to bypass endpoint and email defences entirely, targeting cloud identities, session tokens, and automated workflows. SMBs will need to continuously validate identities, enforce governance, and rebuild trust models across their supply chains to withstand these evolving threats.

MSPs have a strategic opportunity here. By providing identity-aware platforms and educating clients about the specific risks they face, MSPs can differentiate themselves in a crowded market. Effective communication of risk, backed by telemetry and actionable data, will be as important as the technology itself.

Bridging the Awareness–Readiness Gap

The 2025 Guardz survey underscores a recurring theme: awareness is high, readiness is low. SMBs understand the stakes, they know attacks are frequent and potentially devastating, but many lack the resources or expertise to act. Only 34% have formal response plans, 28% rely on informal processes, and 15% have no plan at all.

MSPs can fill this gap, not just with technology but with structured operational support. Guiding SMBs to adopt repeatable processes, maintain updated tools, and implement training programs transforms awareness into actionable readiness. Moreover, MSPs can help SMBs measure risk, enforce policy, and continuously monitor their security posture, actions that are increasingly essential as AI-accelerated threats proliferate.

Practical Steps for MSPs

Based on the report's findings, MSPs should consider the following strategies:

- Adopt an identity-centric security approach: Shift focus from siloed detections to correlating risk across users, sessions, and devices. Identity should be treated as the primary perimeter.
- Consolidate and platformise security tools: Replace fragmented point solutions with unified platforms that automate data correlation, threat detection, and incident response.
- Leverage automation on solid data foundations: Ensure controls, logging, and normalisation are in place to enable AI-powered monitoring and rapid response.
- Educate and guide SMB clients: Provide clear, data-driven insights into risks and mitigation strategies. Make complex security concepts accessible.
- Formalise incident response planning: Help SMBs develop repeatable, testable processes that reduce the impact of breaches and reinforce long-term resilience.

By implementing these strategies, MSPs not only strengthen client security but also position themselves as indispensable partners in an increasingly risky environment.

The Core Message

The cybersecurity landscape for SMBs is changing rapidly. AI-driven attacks, identity-focused threats, and automation have raised the stakes, and SMBs are struggling to keep pace. At the same time, awareness of cyber risk is at an all-time high, signalling that organisations are motivated to act, but they need guidance, expertise, and unified solutions to do so effectively.

For MSPs, this is a pivotal moment. The traditional model of managing a patchwork of client defences is no longer sufficient. Instead, MSPs must embrace consolidated, platform-based security centred on identity, backed by automation and data-driven insights. Those who can bridge the awareness–readiness gap for SMB clients will not only help prevent devastating incidents but will also secure their relevance in a rapidly evolving market.

As Eisner notes, 2026 will likely be the year that identity becomes the frontline of defence. MSPs equipped with unified platforms and strategic guidance will enable SMBs to close critical gaps, strengthen resilience, and confidently face the next wave of cyber threats. The opportunity, and the responsibility, has never been clearer.

Parallel or Just Parallel-ish?

Understanding the real difference - an architectural perspective

BY FLOYD CHRISTOFFERSON, VICE PRESIDENT OF PRODUCT MARKETING, HAMMERSPACE

AS AI and accelerated computing reshape enterprise data strategy, more storage vendors are positioning their architectures as “parallel file systems.” Unfortunately, the term is often applied inconsistently, which creates real challenges for architects trying to distinguish scale-out NAS, distributed object stores, and true parallel file systems.

The term “parallel file system” emerged in the HPC community as massively parallel processors exposed the limits of single-server storage. The idea took shape alongside MPP and hypercube architectures in the late 1980s and early 1990s, as researchers sought storage architectures that could scale with parallel compute. Intel’s Concurrent File System (CFS) demonstrated decluttered storage and concurrent access across I/O nodes, while later research systems such as IBM’s Vesta explicitly framed storage as a parallel service rather than a centralised bottleneck.

These systems helped define a core principle that still holds today: when computation is parallel, storage access must be parallel as well.

What actually defines a parallel file system?

Across HPC, AI, and large-scale analytics, practitioners share a common understanding of what constitutes a parallel file system. At its core, a PFS is a distributed storage architecture in which many clients access data directly and in parallel across multiple storage nodes, based on metadata delivered out of band, within a single shared namespace.

The requirement for direct client-to-storage communication is foundational. In a true parallel file system, clients do not communicate through front-end controllers, NAS heads, or proxy gateways. Instead, they establish parallel data paths to many storage nodes at once, which is what enables performance to scale linearly and predictably as more compute nodes or storage nodes are added.
This principle is not limited to legacy HPC systems; it is used in modern standards-based designs such as Parallel NFS (pNFS), including pNFSv4.2, which is included in all major Linux distributions. With pNFSv4.2, for example, clients receive layout information from a metadata server and then communicate directly with the appropriate storage nodes.
The metadata server coordinates layout state and access, but never proxies data flows: a hallmark of true parallelism.

Metadata out of the data path: The foundational principle

Separating metadata from the data path is perhaps the most essential characteristic of a parallel file system. In a real PFS, metadata is architected so it does not become a serialised bottleneck. Instead, metadata operations are distributed across nodes, delegated to clients, cached intelligently, or orchestrated in parallel. This distinction might sound academic, but its impact on performance is profound. In architectures where metadata and data traffic are

intermingled or where metadata operations pass through controller nodes, concurrency is fundamentally constrained. In contrast, modern PFS designs allow metadata to flow independently from the data, enabling the system to scale horizontally without sacrificing performance. Protocols like pNFS reinforce this by providing layouts out of band while leaving data movement entirely to distributed parallel paths.

Distributed data layout and true parallelism

Parallel file systems also distribute data across many storage nodes in ways that allow clients to access different parts of files in parallel. Whether accomplished through explicit striping, negotiated layouts, or client-driven placement, the result is the same: a system optimised for multi-node, multi-stream I/O at scale.

Crucially, this parallelism arises from direct multi-node access rather than from aggregating performance behind front-end controllers, as is common in scale-out NAS architectures. In a parallel file system, scalability is an inherent property of the data path architecture itself. Adding more controllers to a NAS system may increase aggregate capacity or throughput to a point, but it does not eliminate the architectural limitations imposed by controller-mediated I/O.

Real scalability comes from clients and storage nodes, not controllers

Another distinguishing feature of true PFS architectures is that performance scales directly with the number of clients and storage nodes. If you add more GPU servers and/or storage nodes, aggregate throughput and concurrency increase naturally.

Architectures that funnel I/O through controllers, however, cannot offer this type of scalability. No matter how many backend storage devices they manage, their front-end controllers remain fixed chokepoints. In high-concurrency environments, such as those powering modern AI pipelines, this limitation becomes very quickly apparent.

Metadata architecture is far more important than many discussions suggest

Metadata design is often reduced to overly simple labels like “centralised” or “distributed,” but effective AI and HPC performance requires much more nuance. At scale, metadata must support high concurrency, serve namespace operations in parallel, and enable delegation or client-side metadata caching. And to power modern AI workloads, it must preserve locality across multi-site and multi-cloud environments and ingest metadata from external storage systems into a unified global context.

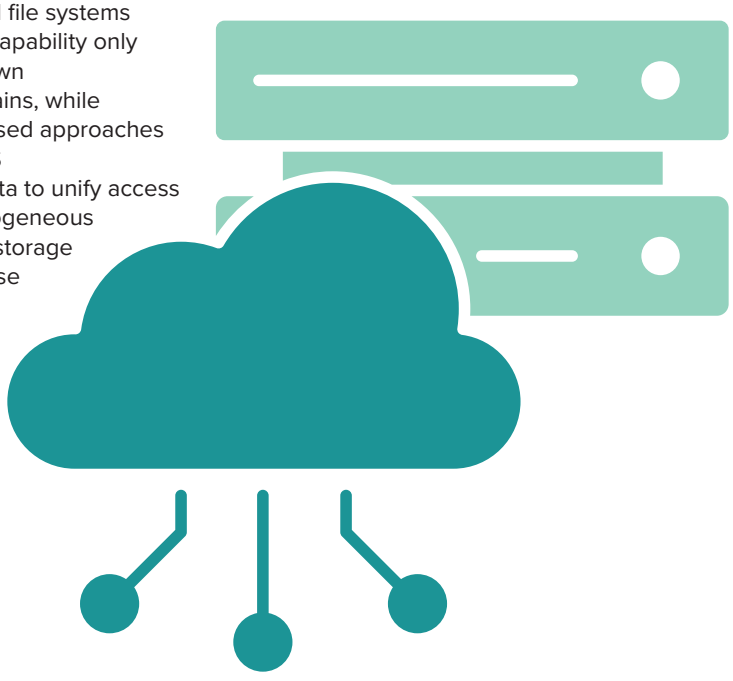
These capabilities matter because AI workloads increasingly span datasets stored across silos, protocols, and geographies. Metadata must operate at global scale without entering the data path, something that favours true parallel file system architectures.

A global namespace does not make a system parallel

Many storage systems now promote the idea of a “global namespace,” but this feature alone does not make a system a parallel file system. A global namespace provides unified visibility and accessibility, but it does not guarantee parallel I/O.

A parallel file system requires both a shared namespace and the architectural ability for clients to access data directly and concurrently across multiple storage nodes, with metadata fully separated from the data path.

Some parallel file systems provide this capability only within their own storage domains, while standards-based approaches such as pNFS allow metadata to unify access across heterogeneous NFS-backed storage systems. These differences significantly affect how useful a global namespace is for AI-scale workloads.



Multiprotocol support is necessary but not sufficient

AI workflows now commonly require both POSIX and S3 access. While many systems claim support for file and object protocols, the architectural model used to deliver that support is critical. In some designs, S3 is access implemented through gateway or controller layers, forcing object traffic through the same bottleneck pathways used for file I/O. In others, object semantics are integrated directly into the distributed parallel architecture, allowing object access to scale horizontally and follow the same direct-to-storage data paths as file access.

As a result, simply supporting file and object protocols is not sufficient for AI-scale workloads if either protocol is funnelled through centralised front ends.

Modern parallel file systems have evolved beyond legacy designs

It is misleading to compare contemporary parallel file systems to early 2000s implementations. Modern designs incorporate distributed metadata services, dynamic layout negotiation, scalable and distributed locking, client-side delegation, parallel namespace operations, and global data awareness extending across multiple sites or storage types.

These capabilities reflect a shift toward AI, interactive, and heterogeneous computing environments rather than the batch-oriented workloads that shaped early HPC systems. The state of the art has advanced significantly.

Controller bottlenecks remain the clearest line between NAS and PFS

One of the simplest ways to distinguish scale-out NAS from a parallel file system is to examine how clients perform I/O. If clients must route data or metadata through controller nodes, regardless of how many controllers exist, the architecture will eventually reach a performance ceiling based on controller CPU and network capacity.

This constraint becomes especially problematic in AI environments where thousands of GPUs generate massive amounts of east-west traffic, where inference workloads require extremely low latency, and where metadata operations must be served in parallel. Parallel file systems avoid these limits by removing controllers from the data path, enabling direct and concurrent client access to storage nodes without any intermediaries.

Rebuild and durability capabilities are no longer differentiators

Many modern distributed systems support advanced erasure coding, parallel rebuilds, and flexible fault domain configurations. While important, these features are now widely available across object stores, scale-out NAS, and parallel file systems. They are not indicators of whether a system is architecturally parallel; they simply reflect the current state of distributed storage technology.

AI workloads extend well beyond training — and stress storage differently

Much of the industry conversation still centres on training benchmarks, but real enterprise AI performance increasingly depends on inference, microservices, agentic AI behaviour, and multi-modal models that require rapid access to diverse data types that may be widely distributed. These workloads involve high fan-out traffic patterns, extreme concurrency, and sensitivity to latency.

Architectures that rely on controller nodes or serialised metadata operations struggle under these patterns. True parallel file systems are well suited to these workloads because they provide direct access paths, distributed metadata management, and high levels of concurrency without introducing centralised bottlenecks.

What modern AI data platforms actually require

In practice, storage systems designed to support AI at scale share a common set of architectural principles. They enable direct, parallel I/O between clients and storage nodes so that bandwidth and concurrency scale with cluster size. They separate metadata from the data path and distribute it in ways that support high levels of parallelism.

At the same time, such modern systems provide unified semantics for file and object access without inserting gateways into critical I/O paths, allowing multiple access models to share the same scalable data plane.

They extend across heterogeneous storage systems, clouds, and sites by unifying metadata rather than confining it to a single physical or vendor-defined environment. They also account for locality within GPU clusters, ensuring that data access aligns closely with the compute fabric.

Finally, modern parallel architectures favour open, standards-based client access over proprietary client layers, enabling broad compatibility and long-term flexibility at scale.

Taken together, these architectural traits define both modern parallel file systems and, more broadly, the storage foundations required to support AI data pipelines effectively.

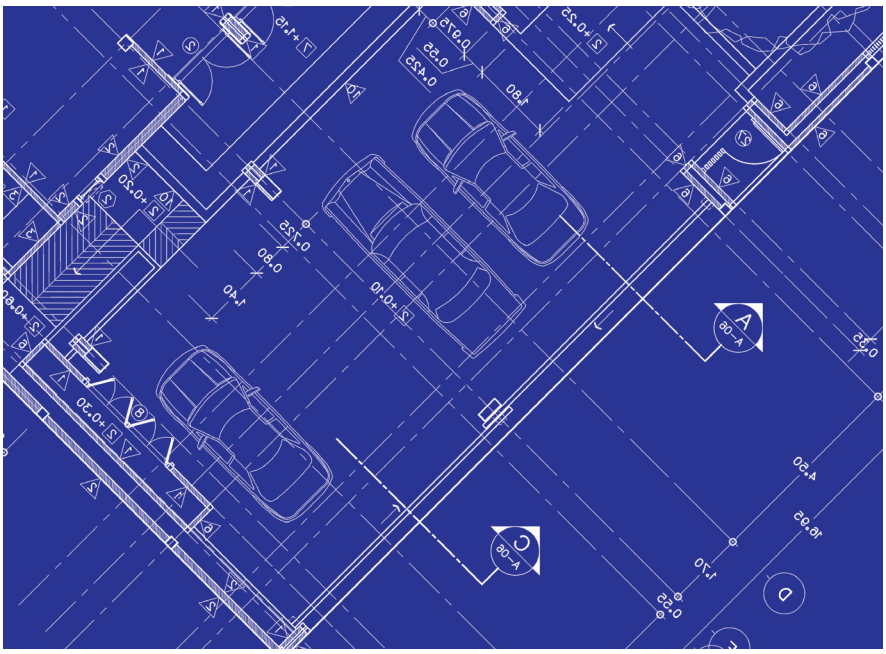
Why true parallelism matters more than ever

A parallel file system is not simply “fast” or “scale-out.” It is an architecture defined by distributed metadata, direct and concurrent client access to storage nodes, and the removal of controller bottlenecks from the data path.

Modern implementations, including those based on open standards such as pNFS, demonstrate how these principles enable scalable operations across heterogeneous, multi-site, and multi-cloud environments.

As AI infrastructure continues to expand, organisations should evaluate technologies based on these architectural fundamentals rather than on labels or marketing terms.

Only systems built on genuine parallelism are best positioned to meet the concurrency, throughput, and latency requirements of next-generation AI workloads.



MANAGED SERVICES SUMMIT

BENELUX
LONDON
NORDICS
MANCHESTER

CREATING VALUE with MANAGED SERVICES

managedservicessummit.com

MANAGED SERVICES SUMMIT BENELUX

benelux.managedservicessummit.com

30 JUNE 2026

MANAGED SERVICES SUMMIT LONDON

london.managedservicessummit.com

09 SEPTEMBER 2026

MANAGED SERVICES SUMMIT NORDICS

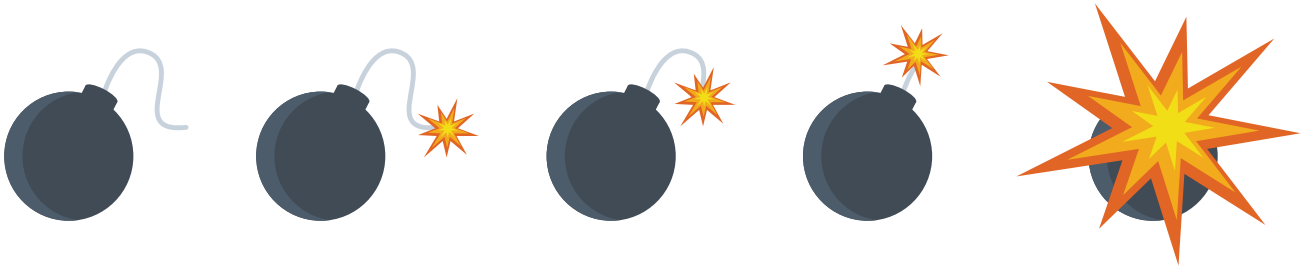
nordics.managedservicessummit.com

05 NOVEMBER 2026

MANAGED SERVICES SUMMIT MANCHESTER

manchester.managedservices summit.com

17 NOVEMBER 2026



AI's Data Privacy Wake-Up Call: Why sensitive data in AI Training is a regulatory and data breach time bomb

BY ROSS MILLENACKER, SENIOR PRODUCT MANAGER, PERFORCE SOFTWARE

MANY DEVOPS leaders could be sleepwalking into a regulatory breach and security nightmare when it comes to AI data privacy. Recent research shows that while most IT leaders focus on locking down production systems, there are very real dangers in non-production environments, such as AI training.

These areas often use real, sensitive data, such as Personal Identification Information (PII), including customer health records, financial information, and Social Security numbers. The consequences can include data breaches, security issues, regulatory fines, and loss of market reputation and customer trust.

Nor are the risks just hypothetical. According to the Perforce 2025 State of Data Compliance & Privacy, 60% of the survey's respondents have experienced data breaches or data theft in software development, testing, AI, and analytics environments, an 11% increase compared to 2024's report results. 22% report regulatory non-compliance status or fines, plus a further 32% have faced audit issues. These results are all the more concerning given that 100% of the survey's 280 global respondents must adhere to regulatory compliance, including CCPA, GDPR, and HIPAA.

Confusion, contradictions, and complacency

While DevOps professionals' awareness of the risks of exposing sensitive data in general may be high, the research shows that this awareness is not translating into safer practices in non-production environments like AI, and that confusion is prevalent.

91% of organisations believe that sensitive data should be allowed in AI training and testing, and 90% use sensitive data in AI.

82% are of the opinion that using sensitive data in AI model training and fine-tuning is safe.

Furthermore, 84% confess to compliance exceptions in non-production environments, including AI, despite the high rate of data breaches, as well as audit and regulatory compliance issues.

Yet, DevOps leaders are not oblivious to the risks being taken:

78% of the survey's respondents admit to being highly concerned about theft or breaches in AI model training.

68% worry about compliance and audit issues.

So why are organisations taking such significant risks? It turns out that the leading reason for 76% of the survey's respondents is data-driven decision-making. Teams working in AI training and other non-production environments like software development, testing, and analytics are data-hungry, depending on information that is as realistic as possible. The further the data drifts away from production-like values, the less accurate the results will be.

Shortcuts win over safeguards

Also, DevOps teams want access to production-like data quickly, which increases the temptation to use real customer data, despite the potential risks of inadvertently exposing sensitive information.

The situation is exacerbated when feeding this information to AI. As most people are increasingly aware, AI is a

blabbermouth that shares secrets and has a long memory.

The reality is that while DevOps leaders know that data privacy is essential, they want to balance that necessity against pressure to innovate as fast as possible, especially in the era of AI. There is also a cultural challenge here: protecting data is viewed as complex, time-consuming, and a roadblock to innovation.

Using real data in AI Is not necessary

It is time to put these misconceptions in their place and remove the confusion. The fact is that there is no need to use sensitive data in non-production environments, by using techniques and tools that deliver realistic fit-for-purpose data. There are also strong indications that, while many organisations might still be a confusing mire today, many have already taken steps towards better protection of data in AI training environments, with other plans emerging.

For example, it is good to hear that 95% have some form of masking policy or mandate, and that 95% are already using static data masking. This method hides or replaces sensitive data while keeping it usable for environments like AI training. Furthermore, modern static data masking tools can provide that data in a fraction of the time it previously took to give DevOps teams realistic production-like data. Whereas once it required database administrators (DBAs) taking days to deliver this data, that timeframe can be brought down to just a couple of hours, and self-served by users, rather than relying on DBAs, some of whose time is subsequently liberated for other priorities.

Another option is synthetic data, which is artificially generated using production-like values, but without having any contact whatsoever with real data. Nearly half of organisations surveyed say they are already using synthetic data in AI development, although adoption is in its early stages: a third report using it on a small scale or experimentally, and a further quarter have tried it but experienced problems with speed, scale, and quality.

Teams will combine synthetic data and data masking

However, synthetic data is evolving at a rapid pace, including the use of AI technology itself to automatically generate realistic artificial data at speed and customised to the situation. Looking ahead, the most likely scenario is that DevOps teams will use a combination of data masking and synthetic data techniques, depending on the use case —for example, for compliance, new applications, or to address a specific requirement.

Looking more broadly, 86% plan to invest in AI-specific data privacy solutions across the next year or so, but it is important to note that tools are not the only answer to better data privacy in AI and other non-production environments. Creating a culture where governance is prioritised and policies are consistently enforced has to be a priority, with awareness and governance part of every DevOps team's DNA.

After all, sacrificing data privacy to keep up with innovation and business demands is a hazardous strategy for DevOps leaders that could end in disaster and with a high price to pay. Conversely, putting in place a plan that gives teams high-quality, production-like data without risking exposure of sensitive data will help DevOps teams maintain, and even improve, innovation at speed and at scale.

From Chaos to Control: The role of frameworks in building resilient cyber security

BY JAMES PRESTON, PRINCIPAL SECURITY CONSULTANT AT ANSECURITY

DAY-TO-DAY, we help companies improve their cybersecurity maturity. It quickly becomes clear what a different view we have to our clients. They often ask us about the GenAI-powered tools and next-gen technologies they've heard so much about from keen marketing teams targeting specific use cases. But, in reality, we're looking for far simpler security controls. Over the countless clients we've worked with over the years - the difference between the resilient and the rest is pretty simple. It's just the basics, implemented to a consistently high standard.

It's the basics that get you

No amount of expensive tooling will save a company from falling afoul of basic oversights. Yet, in the majority of cases this is exactly how these breaches happen. According to the UK Government's Cyber Security Breaches Survey 2024, phishing is used in 84% of the attacks against businesses. Similarly, Verizon's 2024 Data Breach Investigations Report (DBIR) pointed to stolen credentials as the top attack vector in the last year. These are problems that we largely already have solutions for - and yet they continue to be a dogged problem for businesses.

What allows companies to do those basics well? A cybersecurity framework. It really is that simple. In our experience, the mere presence of a framework is by far the biggest differentiator between well-secured and resilient organisations and the rest.

A foundation for good cybersecurity

When approaching cybersecurity, companies have a hard time knowing where to start. What frameworks offer is a guide to good cybersecurity: They offer structure and clarity; achievable milestones and metrics by which to measure success. Above all, however, they offer a playbook - they tell fledgling security programs what their priorities should be and where to start. From there it tells them how to actually measure risk; what metrics to track; where to place controls and invest time and define what is and isn't a priority.

Frameworks install a common language for businesses around cybersecurity. While many may not know how to start implementing security controls in their organisation, frameworks offer them a way. In doing so, they acquire a language to communicate needs to management. This is often an excruciatingly hard thing for many cybersecurity departments who can't find a way to translate technical concerns to business outcomes. In turn, security gets relegated to cost-centre status and departments have a hard time getting necessary budgets or advising on organisational risk. Frameworks provide the metrics and data points necessary to demonstrate how security affects the business, paving the way for longer-term resilience.

Frameworks are also largely scalable, which allows them to work for both small and medium sized businesses (SMEs) - accommodating their security needs as they grow and mature - as well as enterprises. From there, it provides a good basis for growing a business and will allow them to maintain a cybersecurity stance that can accommodate the growth. Indeed, as a business grows and attracts more customers - more will be expected from them - and a framework will help to meet those new expectations.

An easier path to compliance

Even if an organisation isn't committed to its own security - regulators are. Figuring out how to comply with any number of acronymed regulations and accreditations - such as PCI-DSS, GDPR or even Cyber Essentials - is a big headache for businesses. Frameworks offer a paint-by-numbers path to do that and thus avoid the audits, penalties and loss of business that so often accompany non-compliance. If

regulatory audits and investigations do rear their head, companies that use frameworks will have the documented processes needed to demonstrate compliance.

Demonstrating trustworthiness in the supply chain

One of the strongest aspects of frameworks is that certification demonstrates a level of trustworthiness which is hard to gauge in any other ways. Frameworks from recognised bodies such as NIST, ISO 27001, or CIS are brand names and a signal to customers and partners that engagement with a given company won't endanger them.

Companies are right to be concerned - the supply chain is a major source of risk. According to a 2024 Ponemon Institute report, 60% of security incidents emanate directly from vulnerabilities in the supply chain. Many are now expecting the right certifications from potential partners and suppliers. This is increasingly a condition for doing business with other firms. If a firm can't demonstrate that they comply with a given standard or framework, potential partners may forgo doing business with them altogether for fear of introducing third-party risks, or that their association with a non-complying entity endangers their own compliance status.

Frameworks aren't a panacea

There's an easy trap to fall into here. Many will find a framework and merely check its boxes, following its guidance with the mere minimum of effort. While frameworks are effective guides about how to run cybersecurity within an organisation, they must be pursued with intent and discipline. In fact, data from the Center for Internet Security survey shows that 51% reported improvements only after a year, highlighting that frameworks are a long-term investment, not a short-term cure.

Indeed, frameworks aren't a panacea. They won't solve everything in one fell swoop, but they will offer a much-needed path towards greater resilience. They're dependent on a culture which is actively pursuing strong cybersecurity and will likely need buy in from leadership to realise its potential.

Moreover, many businesses will have specific cybersecurity requirements that fall outside of many frameworks' scopes. Companies in the healthcare sector will have specific requirements which a general-purpose framework may not cover. Similarly, industrial firms with large investments into ICS and OT environments will have more specific concerns than many frameworks can offer.

You don't need to trust our word for it: Various studies have confirmed the utility of the cybersecurity framework. One survey from the Center for Internet Security shows that 95% of organisations experienced benefits, 43% reported fewer security incidents and another 43% reported greater maturity in security operations.

Frameworks won't keep out the most advanced, well-resourced attackers - but that's not what most businesses need to worry about. They need to think about how to do the basics well, because it's those small oversights which bring about breaches and regulatory problems. Frameworks provide a way for most businesses to do those basics well and keep out the large majority of threats.

Sorry: To scale development, you have to scale AppSec too

BY NEIL ROSEMAN, CEO, INVICTI

WE'RE LIVING through a boom for software development. One only needs to look at the explosion of global developer populations - which have grown by 50% since 2022. One could also look at projections that say by 2030, the size of the global enterprise software market will double to $517 billion. Or one could simply look around and think about how the world looked only a decade ago. It's now hard to think of an industry that hasn't been profoundly changed by software, or a company that isn't now a "software company."

Software ate the world

As our lives and businesses have moved irreversibly online, demand for new products, services and applications has boomed in parallel. Not only do we want more software, we demand more out of the software we already use, meaning that regular maintenance, improvements, updates and upgrades are now a basic expectation.

Organisations are now looking to make good on those expectations. Everywhere, they're attempting to scale their development efforts to meet this insatiable demand.

Those organisations are not just required to create software, but software that works well and protects its users from abuse. Customers expect it from them and - whether individual consumers or enterprise partners - will surely flee from any provider that doesn't take their security seriously.

On top of that, national, international and sectoral regulations increasingly demand that users be protected and will punish those that don't respect that basic expectation. That said, while enterprises are rapidly scaling their development efforts, they're often not scaling their AppSec efforts in parallel.

Uneven scaling

Even in times of lesser demand, software development regularly exposed vulnerabilities and bugs to end users. As organisations try to step up their development efforts, these problems don't just scale but become disproportionately problematic as they put stress on the AppSec functions which previously kept vulnerabilities in check.

In fact, Cypress Data Defense's 2025 State of Application Security report shows that 62% of organisations actually release insecure code, knowing it to be insecure, in order to meet deadlines.

Furthermore, the increasing demand for new software has forced developers to rely ever more on AI tools and open-source libraries. Indeed, vibecoding practices have taken root in software development in response to that increased pressure.

But with the increased ease and scale that vibecoding and AI tools grant, developers also lose meticulous awareness about their build decisions and the security of their code, thus potentially accelerating the production of vulnerabilities. Furthermore, open-source libraries continue to be a common and serious source of risk for applications

But with the increased ease and scale that vibecoding and AI tools grant, developers also lose meticulous awareness about their build decisions and the security of their code, thus potentially accelerating the production of vulnerabilities.

Furthermore, open-source libraries continue to be a common and serious source of risk for applications. In fact, one paper says that reported vulnerabilities in open-source components have grown by 98% annually over the last few years and that there had been an 85% increase in the average lifespan of those vulnerabilities, indicating that although vulnerabilities were known about, they were often being ignored.

The problem with scaling development efforts is that AppSec needs to be scaled in kind, or so much pressure will mount on development that bugs and vulnerabilities will flow through unhindered.

In fact, Verizon's 2024 Data Breach Investigations Report highlighted that between 2023 and 2024 - businesses experienced a 180% increase in the exploitation of software vulnerabilities as a path to breach. This can be at least partially explained by the huge expansion that many organisations have made in development without a parallel expansion in AppSec. That's a reality that many enterprises now need to understand.

Tipping the scales towards insecurity

The basic first problem that many enterprises who scale development without scaling AppSec will run into is a simple growth in the risks to software - inviting more bugs, vulnerabilities and then breaches. For a business that can't secure its apps, that will likely mean a loss of customer faith. If customers find their releases embedded with vulnerabilities and bugs - they will start looking elsewhere for a more secure software provider. Worse yet, if those customers experience security incidents through their software providers - that will only hasten their flight from their erstwhile provider. Furthermore, their costs for fixing problems after deployment will quickly balloon as bugs often cost multiple times more to fix after production than before.

Those might be acceptable losses for some, but mature AppSec is increasingly becoming a competitive differentiator, a baseline compliance requirement and a condition for engagement with other businesses.

The lash of the supply chain

The effects of insufficient AppSec spread far and wide. We now live in a technological age in which we are all deeply interlinked.

In August this year, attackers got their hands on Salesloft OAuth tokens, stolen through the integration with Salesloft's Drift chatbot. They then used those tokens to compromise over 700 organisations including cybersecurity firms such as Palo Alto Networks and Cloudflare. Attackers accessed highly sensitive data too, including embedded secrets like API and AWS keys. They didn't even have to exploit a vulnerability in Salesloft's core platform, but the insecure application integration between the chatbot and Salesloft. This case is another example of how poor AppSec in one place can lead to catastrophic compromises in countless others.

Recognising that threat, efforts are now being made to police each link in the supply chain. What's more is that enterprise customers can now closely scrutinise the software they're using and make crucial decisions based on their partner's releases. The rise of the Software Bill of Materials (SBOM) is a great example of that. Now customers can inspect and analyse the basic components of software releases and hold developers to account. That new scrutiny that customers are now capable of should make good AppSec a real priority for businesses, especially considering they might lose customers because of it. Increasingly, SBOMs are now becoming a basic requirement for engagement with many enterprises and governments.

Similarly, regulation is also demanding increasing scrutiny over third parties and the supply chain as a whole. The EU Cyber Resilience Act will come into force in 2027 and will fine businesses up to 15 million for non-compliance. Aimed at tackling the cyber resilience of the EU holistically, this act demands the use of SBOMs in all digital products within the EU and update them regularly so that customers and partners can stay abreast of the contents of the software they're using.

More recently, the Digital Operational Resilience Act (DORA) came into enforcement in the EU's financial sector. This landmark regulation will make compliant entities responsible for the risk profiles of their partners and potentially liable for the failures in their supply chain. For many of those who supply to the EU financial sector - one of the world's largest financial markets - high AppSec standards will become a crucial competitive differentiator.

In multiple ways, AppSec is becoming an unavoidable duty for companies. To be sure, it should always have been in the first place, if only to ensure the security of its customers and partners. However, even those who overlook their AppSec responsibilities will soon be compelled to adjust or risk losing business and revenue to regulatory penalties and falling customer faith.

The solution, however, is for companies to stop seeing their application security processes as a costly appendage and start seeing it as a central part of their development efforts and a means of ensuring their products' long-term success.

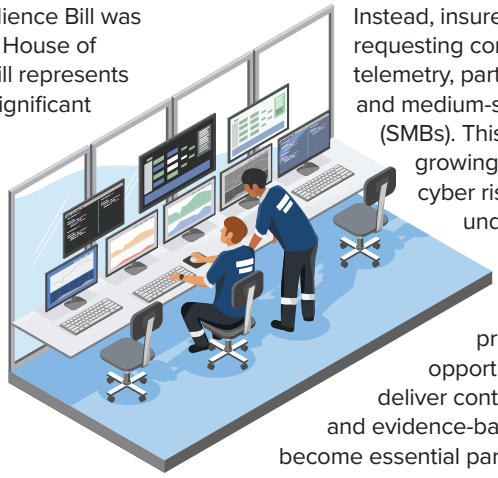
The channel in 2026: How 2026 will be a defining year for MSPs

BY JAMIE AKHTAR, CEO AND CO-FOUNDER OF CYBERSMART

BY THE END of 2026, the managed service provider (MSP) market will look fundamentally different from that of today. The shift will not be driven by technology alone, but by regulation, insurance, board-level scrutiny and supply-chain pressure too. Critically, MSPs will sit at the centre of the UK's cyber resilience ecosystem and will be expected to prove it every day. But which changes will affect MSPs the most?

Introduction of the UK's cyber security and resilience bill

The most visible catalyst is regulation. In November 2025, the UK's Cyber Security and Resilience Bill was introduced to the House of Commons. The Bill represents one of the most significant government-led cybersecurity reforms in recent years. Once enacted, the Bill will broaden both the definition and the responsibilities of 'Relevant Managed Service Providers,' bringing an estimated 1,000 MSPs directly into scope, particularly those supporting critical national infrastructure (CNI) or public sector-linked organisations. Adoption of the Cyber Assessment Framework across critical sectors will introduce clearer expectations around baseline security controls, incident reporting and formal assurance. For many MSPs, this marks a transition from being indirectly affected by regulation through clients, to being regulated entities in their own right, under the banner of the new Information Commission (IC).



This change matters because it resets the relationship between MSPs, customers and regulators. Transparency and discipline will no longer be optional differentiators; rather they will be critical stakes. Recent research suggests that the market is already moving in this direction, with 77% of MSPs reporting the increased scrutiny of their security capabilities by prospects and customers over the past year. By 2026, that scrutiny will be systematic, continuous and often externally enforced.

Real-Time operational risk becomes key insurance indicator

Insurance will play a parallel role in accelerating this shift. The cyber insurance market is moving away from static, point-in-time questionnaires that fail to reflect real operational risk. Instead, insurers are increasingly requesting continuous security telemetry, particularly for small and medium-sized businesses (SMBs). This reflects a growing consensus that cyber risk can only be understood through real-time visibility. For MSPs, this creates both pressure and opportunity. Those able to deliver continuous monitoring and evidence-based assurance will become essential partners in helping customers secure cover at viable premiums. Those that cannot will find themselves excluded from deals before conversations even begin.

Board expectations will rise sharply

At the same time, board-level expectations are rising sharply, with cybersecurity fast becoming an essential board discussion. Directors are no longer satisfied with policies, frameworks or certifications that look impressive but cannot be demonstrated in practice. This shift coincides with the increasing media attention given to high-profile hacks, especially those that have led to significant financial and reputational losses. No doubt board members have stood up to the potential risk and devastation of a cyber incident. Now, boards need verifiable proof of operational cyber hygiene, including controls that are implemented, monitored and effective on a day-to-day basis. This is driving rapid adoption of automated evidence collection and continuous control monitoring, replacing annual compliance exercises with living assurance models. By 2026, MSPs will increasingly be judged not on what they say they do, but on what their data shows they are doing right now.

Increased supply-chain scrutiny

Supply-chain security will complete the picture. High-profile interventions such as the FTSE 350 cyber letter and updated defence requirements under CSM v4 have pushed cyber resilience firmly into mainstream procurement. Cyber resilience is now a normal, expected and enforceable part of how organisations select and retain suppliers, not a specialist conversation reserved for security teams or high-risk contracts. Large organisations now expect their suppliers, including SMEs supported by MSPs, to demonstrate consistent, certifiable cyber controls. This pressure flows downstream, making MSPs key enablers of supply-chain compliance. In practice, this means MSPs must standardise security baselines across their customer base, ensuring resilience is not bespoke or ad hoc, but repeatable and provable.

Key Takeaways: The MSP in 2026

Between increased regulation, scrutiny and dependence, MSPs will evolve from trusted IT partners into regulated cyber operators. Success will depend on their ability to provide continuous assurance, real-time visibility and demonstrable resilience, not just for clients but for themselves. Whilst there's no enforcement date yet, those who adapt early will find regulation, insurance and supply-chain demands reinforcing their value. Those who delay will discover that the market no longer rewards intent, only evidence.

MANAGED SERVICES SUMMIT

BENELUX
LONDON
NORDICS
MANCHESTER

CREATING VALUE with MANAGED SERVICES

managedservicessummit.com

MANAGED SERVICES SUMMIT BENELUX

benelux.managedservicessummit.com

30 JUNE 2026

MANAGED SERVICES SUMMIT LONDON

london.managedservicessummit.com

09 SEPTEMBER 2026

MANAGED SERVICES SUMMIT NORDICS

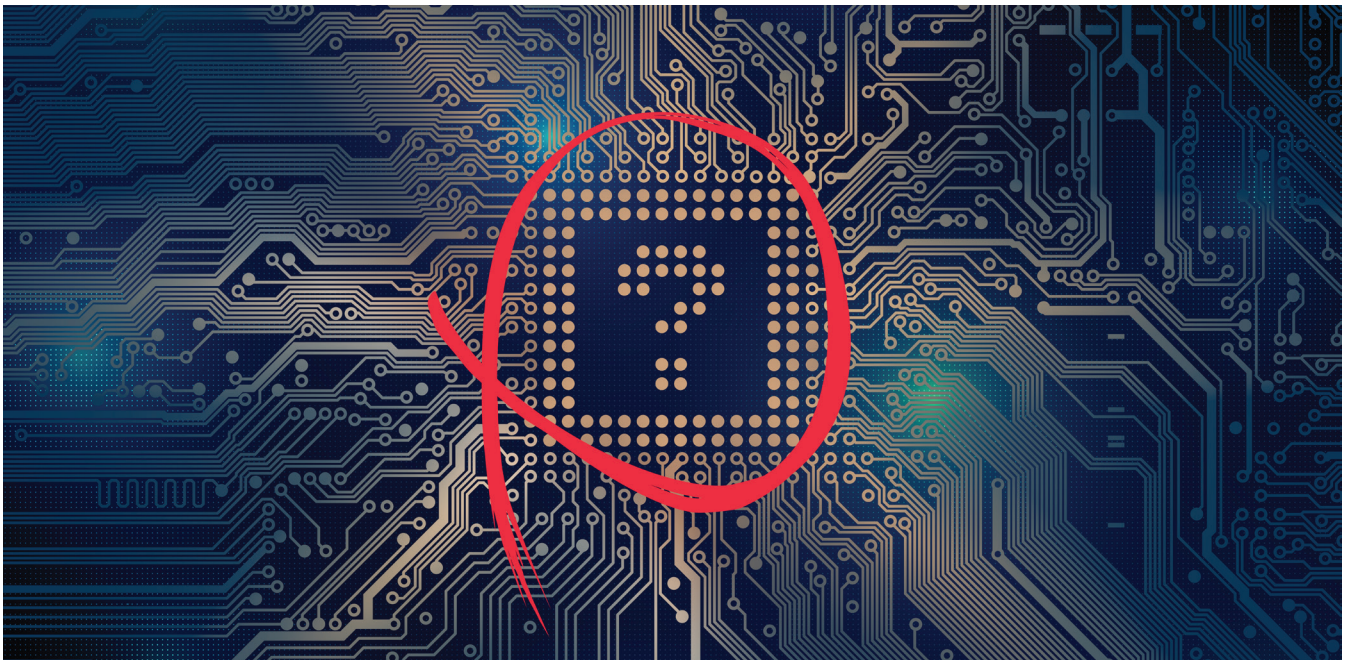
nordics.managedservicessummit.com

05 NOVEMBER 2026

MANAGED SERVICES SUMMIT MANCHESTER

manchester.managedservices summit.com

17 NOVEMBER 2026



AI's growing pains reveal how sustainable IT can solve hardware shortage

BY PETER MILLER, SALES MANAGER AND REFURBISHED TECHNOLOGY EXPERT AT ETB TECHNOLOGIES

AS AI ADOPTION accelerates, the global IT hardware market finds itself in uncharted territory. The demand for high-performance computing equipment – especially GPUs, CPUs and memory components – continues to outpace supply at a speed not seen since the pandemic-era supply chain collapse.

For data centres, MSPs and IT decision-makers, the question is no longer if hardware scarcity will impact operations, but how to stay agile when it does.

The AI acceleration and its ripple effect

AI has shifted from an emerging capability to a fundamental driver of innovation across every sector. From predictive analytics in manufacturing to content generation in media, the appetite for processing power is relentless. NVIDIA reported a 154% year-on-year increase in data centre revenue in 2024, largely driven by demand for AI workloads. But that same growth has squeezed global supply chains, creating long lead times and volatile pricing across the secondary market.

At the same time, energy efficiency and sustainability targets are reshaping how organisations think about IT infrastructure. The convergence of these pressures, including performance, availability and environmental responsibility, is forcing decision-makers to rethink traditional procurement models.

Lessons from past supply chain crises

The pandemic exposed just how fragile global supply chains could be. Businesses dependent on just-in-time inventory found themselves paralysed as lead times for critical components ballooned. Those who fared best were the ones who had built flexibility into their procurement strategies, diversifying suppliers, leveraging alternative markets and extending the life of existing assets.

Today's AI-driven shortages echo those same challenges. Relying solely on new equipment pipelines can leave organisations vulnerable. By contrast, those who plan for variability, through smarter forecasting, lifecycle management and sustainable sourcing, are better positioned to maintain operational resilience.

The strategic role of refurbished IT

Refurbished hardware has evolved far beyond the perception of being a "stopgap" measure. Quality-assured refurbished servers, storage arrays and networking components now offer comparable performance to new equipment, often at a fraction of the cost and delivery time.

Increasingly, businesses are viewing refurbished IT not as a compromise but as a strategic advantage. It allows them to scale quickly, bridge supply chain gaps and deliver on sustainability goals without sacrificing reliability. The global market for refurbished IT equipment is set to grow by more than 12% annually by 2027, driven by data centre demand and corporate environmental targets. In an environment where GPU scarcity can delay AI deployments by months, refurbished alternatives provide a critical lifeline for continuity and greater innovation.

Agility through smarter buying

Navigating ongoing hardware constraints demands a more nuanced approach to procurement. Agility now depends on a willingness to balance performance needs with availability and total cost of ownership.

One part of that equation is embracing multi-source procurement strategies. By diversifying between authorised resellers and trusted refurbishment partners, organisations reduce dependency on a single supply route and gain flexibility when market pressures shift. Another is recognising that existing infrastructure often has more to give. With proper maintenance, upgrades and support, many systems can continue to perform at a high level for years beyond their projected lifecycle, delivering both economic and environmental returns.

Sustainability has become a key factor in procurement decisions. Circular economy principles are no longer a niche concern but a competitive differentiator. Choosing refurbished hardware supports carbon reduction commitments while also strengthening supply resilience. Crucially, this approach must be underpinned by strong partnerships. Working with experienced refurbishment specialists ensures quality assurance, compatibility, and post-sale support that matches or exceeds expectations set by new equipment suppliers.

The cost of inaction and a smarter path forward

Delaying procurement decisions or waiting for supply constraints to ease can prove costly. Beyond the financial impact, it can slow innovation, restrict scalability and undermine competitiveness.

The pace of AI adoption means that organisations unable to secure or optimise their infrastructure risk being left behind.

The IT landscape is changing, and so too must the approach to building and maintaining infrastructure. As AI continues to reshape demand patterns, organisations that think smarter about procurement will be the ones that thrive.

By combining flexible sourcing, sustainable practices and strategic refurbishment, businesses can stay ahead of both technological and market shifts. The future belongs to those who view supply challenges not as obstacles, but as opportunities to innovate.

Protecting MSPs from human-centric cybercrime

BY CARL WEARN, HEAD OF ANALYSIS AND FUTURE OPS AT MIMECAST

MANAGED SERVICE PROVIDERS (MSPs) sit at a critical point in today's cyber landscape. Not only are they service providers, but they are also responsible for protecting the digital element of an organisation.

Their privileged access to multiple client environments makes them a highly attractive target for cybercriminals. Just as supply chains are attacked to maximise reach, breaching an MSP offers attackers a direct path into many different organisations at once. For cyber criminals, the prize for breaching an MSP is high given the amount of data they hold.

Pain points facing MSPs

Unlike larger organisations with dedicated security budgets, MSPs often operate under tight financial constraints. They compete in a crowded market where customers frequently prioritise cost over comprehensive security. At the same time, their staff are stretched thin, asked to balance proactive defence with constant firefighting.

This environment creates a perfect storm of challenges. Limited resources make it difficult to provide ongoing training or continuous monitoring. Budget pressures mean that clients often resist additional spending, even when the risks are clear, leaving MSPs hesitant to invest further without a visible return. Reputational damage is also a major concern. A single breach can ripple across multiple clients, amplifying its impact and undermining trust.

Human risk compounds these pressures. Helpdesk and support staff often sit at the frontline of client interaction, handling urgent requests and resolving issues quickly. This pace, combined with the privileged access many MSP employees have to customer environments, makes them attractive targets for phishing, social engineering and MFA fatigue attacks. For a busy or under-resourced MSP, even a momentary lapse can open the door to a serious compromise.

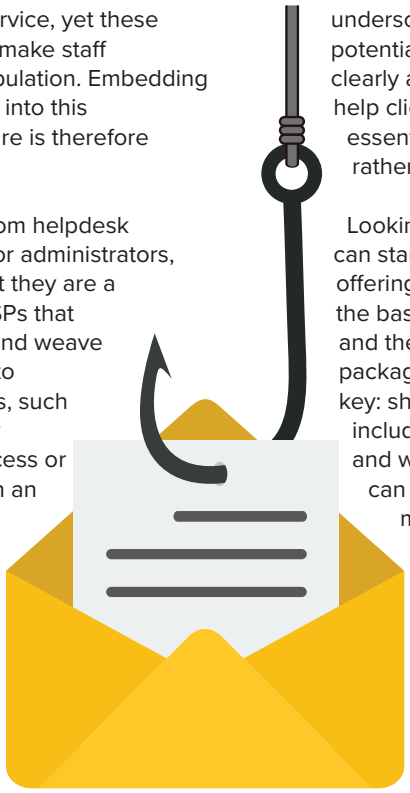
This combination of limited resources, elevated risk and heavy responsibility means MSPs must think differently about security. Protecting their own staff and changing internal culture is just as important as deploying technical defences for clients.

Building a security-first culture

Defending against human-centric attacks requires a cultural shift within the MSP itself. Cybersecurity cannot sit solely with the security lead or IT director; it must be a shared responsibility across the entire workforce. MSPs rely on speed, responsiveness and trust to

deliver excellent service, yet these same qualities can make staff vulnerable to manipulation. Embedding security awareness into this service driven culture is therefore essential.

Every employee, from helpdesk technicians to senior administrators, must recognise that they are a potential target. MSPs that acknowledge this and weave security thinking into everyday workflows, such as verifying identity before granting access or pausing to question an unusual client request, are better positioned to mitigate human-centric risks. Fostering this kind of cultural resilience is not about fear but rather empowerment. Effective training should focus on recognition and response, such as spotting suspicious login requests, pausing before resetting a password or verifying financial instructions through a secondary channel. To be effective, training must evolve beyond compliance checklists and become a regular part of operational life.



Embedding this change will not happen overnight. MSPs need to give their teams permission to slow down, verify and escalate without fear of blame or delay penalties. Security must become part of daily conversations, not a once-a-year compliance exercise. MSPs that achieve this shift will be better protected internally and more credible when demonstrating their security posture to clients.

Selling security in a cost-conscious environment

Unsurprisingly, budgets remain a barrier to enhancing security. Both MSPs and their clients may view security as something to minimise rather than invest in.

Yet in today's environment, security is revenue protection. The recent Marks & Spencer cyber-attack, reportedly costing the business £300 million, underscores the scale of potential loss. MSPs that can clearly articulate this reality can help clients see security as essential to business resilience rather than an optional extra.

Looking practically, MSPs can start by tiering security offerings, so clients understand the baseline level of protection and the benefits of enhanced packages. Transparency is key: show clients what is included, what risks remain and what additional services can mitigate them. This makes upselling less about pressure and more about informed choice. MSPs that demonstrate strong internal practices from robust verification, transparent processes and visible staff awareness, enhance their own credibility and make a stronger case for investment.

Training MSP staff on social engineering

Of all the attack methods, phishing remains the most successful. Business email compromise, fraudulent password reset requests and MFA fatigue attacks are designed to exploit the helpfulness and speed that make MSP teams effective.

Training is essential, but it must be frequent, and scenario-based. Staff need to see realistic phishing simulations, hear examples of how attackers manipulate trust and practice escalation procedures. If an engineer pauses before granting a reset, or if a helpdesk worker checks with a colleague before approving unusual access, that hesitation can stop an attack in its tracks.

Practical steps forward

To reinforce their defences, MSPs should prioritise strengthening identity verification, even if it introduces small delays. Monitoring human risk, such as repeated login issues or frequent password resets, can help identify areas where extra support or training is needed.

Investing in continuous, scenario-led awareness training builds reflexive caution, while strong email filtering reduces the number of threats that reach staff in the first place. When breaches do occur, robust backup, recovery and incident response processes ensure resilience. Positioning resilience as a managed service offering also creates a new opportunity for MSPs to add value.

The opportunity for MSPs

The reality is that cybercriminals target people because people are often the weakest link. For MSPs, this reality brings both risk and opportunity.

By recognising human behaviour as the new frontline, embedding cultural change and reframing security as business protection, MSPs can strengthen their defences and differentiate themselves in a crowded market.

Ultimately, the MSPs that succeed will be those that treat security not as a cost but as the foundation of trust. In a world where attackers are exploiting people as much as technology, that trust is the most valuable service an MSP can provide.

Fostering this kind of cultural resilience is not about fear but rather empowerment. Effective training should focus on recognition and response, such as spotting suspicious login requests, pausing before resetting a password or verifying financial instructions through a secondary channel. Ultimately, the MSPs that succeed will be those that treat security not as a cost but as the foundation of trust

Beyond Visibility: Why continuous monitoring is now the MSPs' first line of defence

BY EDWARD KNIGHT, DIRECTOR GLOBAL MSP SALES, PAESSLER GmbH

THE ROLE OF the managed service provider has fundamentally changed. Organisations no longer want someone who simply reacts when something breaks; they expect a strategic partner who can anticipate issues and stop them before they impact operations. That expectation is reshaping how MSPs think about network oversight and security.

The notion of a fixed network perimeter has disappeared. Hybrid environments, cloud-first architectures, remote workforces, and a growing ecosystem of connected devices have dissolved the boundaries that once defined corporate networks. In this new reality, visibility isn't an optional add-on. It has become the *de facto* security perimeter.

This article explores how continuous monitoring equips MSPs to strengthen resilience while simultaneously reducing compliance exposure and operational risk.

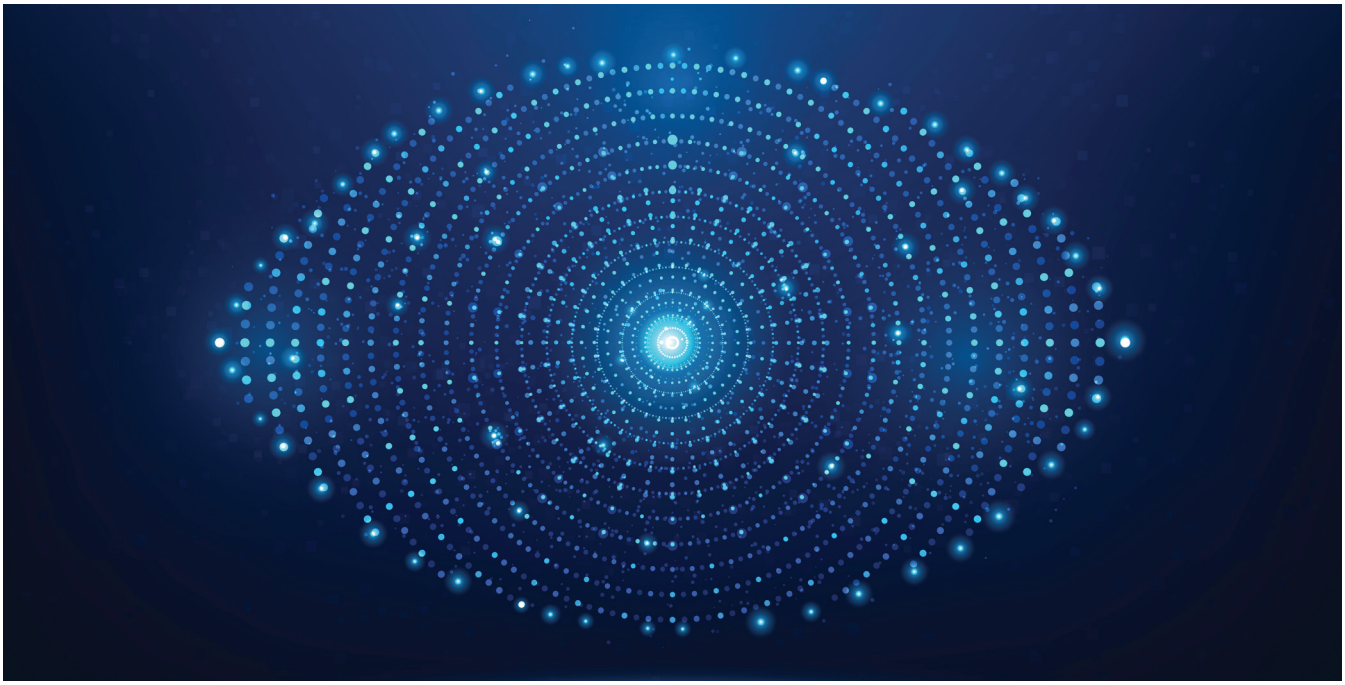
From reactive to proactive defence

In an increasingly distributed and complex environment, visibility has become the first line of defence. Without comprehensive insight into every connection, device, and user activity across a client's network, MSPs are essentially flying blind. Continuous monitoring provides holistic insight, transforming what was once a reactive troubleshooting tool into a proactive security layer.

This distinction highlights the changing nature of IT. Where once reactive detection would suffice, we now expect the proactive - an unexpected external server, abnormal data transfer patterns, or authentication attempts from unfamiliar locations - to be captured before they can escalate.

This proactive stance requires a different operational mindset. Rather than waiting for alerts to trigger action, MSPs need systems that baseline normal network behaviour and flag deviations automatically. Pattern recognition becomes critical: understanding what normal looks like for each client environment makes it possible to spot the abnormal quickly and accurately.

As well as reducing the risk of security breaches, this helps mitigate compliance challenges. A single data breach can result in significant fines, legal costs, and reputational damage that far exceeds the investment in preventive monitoring. MSPs that can demonstrate measurable risk reduction and compliance support find



themselves in a stronger position when competing for contracts, particularly in regulated sectors like finance, healthcare, and professional services.

Consolidation as a strategic advantage

Consolidating monitoring capabilities onto a single, flexible platform addresses several challenges simultaneously. It reduces operational complexity, eliminates gaps in visibility, and provides teams with one trusted source of truth when investigating potential threats. For MSPs managing dozens or hundreds of client networks, this consolidation translates directly into faster threat detection and more efficient resource allocation.

Unified monitoring also supports better client communication. When MSPs can demonstrate comprehensive visibility and show clients exactly what's happening across their infrastructure, it builds confidence and justifies the value of managed services. Transparency becomes a competitive differentiator in a crowded market where many offerings appear similar on paper.

AI, automation, and the human element

Artificial intelligence and automation are reshaping threat detection capabilities. Machine learning algorithms can process vast amounts of network data, identify patterns, and flag anomalies far faster than manual analysis allows. For MSPs managing multiple clients, this speed and scale are essential.

However, the best MSPs pair these technological capabilities with human expertise and contextual understanding. An automated alert about unusual network traffic might indicate a genuine threat, a legitimate business activity, or a misconfigured application. Human judgement determines which scenarios require immediate action and which need further investigation.

Clients don't expect their MSP to simply forward automated alerts. The MSPs that succeed are those that use technology to enhance their team's capabilities rather than replace customer service.

Trust: The MSP market's defining advantage

In a market where technical capabilities are increasingly commoditised, trust is the primary differentiator. Clients choose MSPs they believe will protect their interests, communicate honestly about risks, and deliver simple and measurable outcomes.

By providing ongoing visibility into network health and security posture, MSPs can demonstrate consistent value rather than only during crisis moments. Regular reporting on detected and prevented threats, compliance status, and infrastructure performance builds confidence and reinforces the partnership.

For UK MSPs navigating cost pressures and compliance requirements, continuous monitoring is not simply a technical capability, it's a business strategy that supports sustainable growth, stronger client relationships, and genuine competitive advantage in an increasingly crowded market.

The all-in-one platform trap: why depth, not just breadth, wins for MSPs

BY PETE WILSON, SENIOR DIRECTOR, CHANNEL SALES EMEA, ILLUMIO

THE MOVE toward all-in-one platforms feels unstoppable. Organisations are being drawn into consolidating with single vendors to simplify management, reduce procurement friction, and bring everything under one roof. The appeal is obvious – predictability, convenience, and the reassurance that comes from standardising on a trusted brand.

But for MSPs, this trend creates both an opportunity and a hidden danger.

While having fewer tools to manage can sound appealing, breadth rarely equals depth. In my experience, many businesses assume that because such a platform includes a security suite, they're automatically protected. But just because it's all under one roof doesn't mean every requirement is covered.

That misplaced confidence can create dangerous blind spots, and it's here that MSPs have an essential role to play in restoring balance.

When consolidation creates risk

One of the biggest misconceptions I see in enterprise security is the belief that if a capability is included in a licence, it must be good enough. That mindset is fine for most IT support tools, but it's dangerous when it comes to solutions that are relied upon to protect the business from cyberattacks.

The reality is that all-in-one platforms often offer broad coverage at the surface level but lack the depth required to detect, contain, and disrupt real-world attacks. This is particularly true inside the network, where attackers move after gaining initial access. East–west traffic, where lateral movement, ransomware propagation, and insider threats unfold, is the area most overlooked by broad platforms. Yet it's where attacks do the most damage.

Our latest research found that despite widespread adoption of cloud detection and response tools, 90% of security leaders experienced lateral movement incidents in the past year. On average, each incident caused more than seven hours of downtime and cost organisations around $227,000.

And for MSPs, those gaps become service risks. When a bundled tool lacks the depth to detect or contain real-world attacks, it's the MSP, not the platform vendor, that carries the operational burden, the emergency weekend work, and the client frustration that can end a contract.

Beyond security gaps, platformisation creates a second problem: it makes differentiation nearly impossible. If every MSP leads with the same platform, the market becomes flat. Services begin to look identical, margins shrink, and customers struggle to tell one provider from another. In a fiercely competitive market, MSPs cannot afford to be reduced to licence fulfilment. The partners who win are those who

position themselves as strategic advisors, not resellers.

Why specialist tools still matter

When it comes to cybersecurity, agility and depth matter more than breadth. Platform vendors inevitably evolve on slower release cycles, tied to roadmaps that prioritise stability and scale over innovation. Specialist security providers, by contrast, tend to push boundaries faster and do better with adapting to new attack techniques.

Segmentation is a prime example. Whilst platforms may claim basic traffic controls, true segmentation requires granular policy enforcement that can contain ransomware or lateral movement in real time - something broad suites rarely achieve with the same precision or speed.

Shifting from tools to outcomes

The problem is too many customer conversations still begin with the wrong question: "What tools do we already have?"

It's an understandable starting point, especially when budgets are tight and enterprise licences bundle in so many security features. But focusing on what's included misses the point. Security should be framed as an outcome, not a features list.

I encourage partners to reframe these discussions around the results their customers need: better visibility, faster containment, greater resilience. Starting from outcomes naturally moves the conversation from selling tools to solving problems. If your customers are only asking what's in the bundle, you're not addressing their challenge. The real question is: "What are we trying to achieve?"

This shift changes the partner's role completely. Rather than acting as resellers, MSPs become trusted advisors who align technology decisions with risk reduction, compliance, and business continuity. That's where true value lies – not in the stack itself, but in the confidence it delivers.

Integration as a differentiator

The real opportunity for MSPs isn't choosing platforms over specialists or vice versa, it's integration. That is, stitching together platforms and specialist tools to build secure, outcome-driven architectures that customers can't get anywhere else.

The most successful partners I see are those who take the time to understand how each layer of technology interacts, then tune and optimise those integrations to deliver measurable resilience.

This is especially true for strategies like Zero Trust and breach containment, which typically require multiple specialist vendors offering complementary capabilities. Being able to curate the right selection of platforms, specialist tools, and services to create a single cohesive strategy, as well as matching it to each customer's unique IT environment and business needs, is where MSPs can really prove their worth.

Making platformisation safe for business

For most MSPs, consolidation is now a customer expectation. All-in-one platforms promise simplicity, fewer vendors to manage, and predictable licensing. But the more customers collapse their security stack into one ecosystem, the harder it becomes for MSPs to differentiate, and the greater the risk that essential controls get lost in the gaps.

The role of MSPs is to make platformisation safe, ensuring customers gain the benefits of consolidation without inheriting its blind spots. It's not about abandoning platformisation, but guiding it, leveraging best-in-class technology where appropriate to build an environment that supports a unified view without sacrificing critical control.

By combining the reach of major platforms with the depth of specialist expertise and tools like segmentation, MSPs can build architectures that are both agile and resilient. Platformisation isn't the enemy – complacency is. The partners who help customers balance convenience with control, and who add depth where platforms only offer breadth, will be the ones who earn trust, demonstrate true value, and secure a lasting competitive advantage in the market.

Momentum over noise:
What MSPs really need from 2026

THERE IS NO shortage of noise in the channel right now. Big announcements. Big claims. Big promises about AI, transformation and the next wave of opportunity.

What there is less of is patience.

That was the unspoken context behind Gamma's recent Partner Kick Off webinar, hosted by Will Morey and joined by Andrew Belshaw, Group CEO of Gamma, Colin Lees, CTO, John Murphy, CEO of Gamma Business, and Matt Townend from Cavell.

The format was deliberately informal, but the message was not. MSPs are done being sold the future. They want help dealing with the present, and a clear line of sight to what works next.

2026, the panel agreed, is not about hype. It is about momentum. And momentum only comes from delivery.

"Partners are not looking for more promises. They are looking for clarity and certainty."
Will Morey, Managing Director, Gamma Business

The market has changed. Expectations have too

It was agreed that 2025 had been one of the most uncomfortable years the channel has faced. Economic uncertainty, political instability, the PSTN switch off accelerating, AI complicating technology decisions rather than simplifying them.

Against that backdrop, MSPs are being pulled in multiple directions at once. Protecting existing revenue. Managing migration. Winning new business. Upskilling teams. All while customers expect more and are willing to tolerate less disruption.

What came through clearly is that partners are not asking vendors for inspiration anymore.

They are asking for reliability. They want suppliers they can trust to still be here in five years' time, and platforms they can build around without constantly revisiting decisions. Trust, in this context, is not a brand value. It is commercial risk management.

Why the unglamorous stuff matters more than ever

A recurring theme was the idea of value below the surface. The things customers rarely see but MSPs feel every day. Resilience. Security. Compliance. Service reliability. The operational reality of running platforms at scale.

Anyone can sell features.

Far fewer can fund the engineering, infrastructure and support needed to keep those features working properly over time. In a maturing market, that difference is becoming harder to ignore.

"Anybody can talk about what sits above the waterline. What matters is how secure, resilient and consumable it is underneath."
Andrew Belshaw, Group CEO, Gamma

This matters even more as regulation tightens and AI increases the attack surface. MSPs are being asked harder questions by customers, auditors and, increasingly, potential investors. Platforms that are not secure or compliant by design will be exposed eventually.

AI has moved from excitement to accountability

Perhaps the most important shift discussed was the changing role of AI. Twelve months ago, AI was still a differentiator. Now it is on trial. MSPs are no longer interested in AI for AI's sake. They want to know whether it reduces tickets, improves response times, helps agents do their jobs better, or creates sellable services without requiring specialist headcount. Anything that adds complexity without delivering operational benefit is quietly being deprioritised. The same applies to CX. There is real opportunity there, but only if it can be delivered in a way that fits how MSPs work.

"AI is now at a point where it has to earn its place. It has to make a real difference, not just sound impressive."
Colin Lees, CTO, Gamma

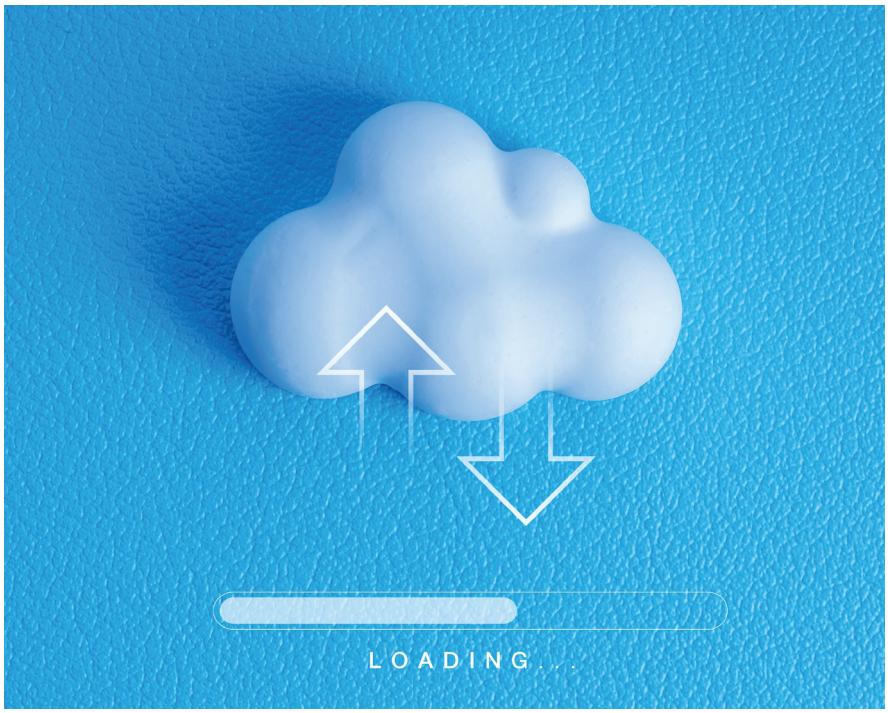
Choice without chaos

One of the more practical discussions centred on UCaaS and the importance of choice that does not create confusion. Different customers need different outcomes. Some are price-led. Others are security driven. Others want transformation.

MSPs need the flexibility to meet those needs without rebuilding their sales and support model every time. The direction of travel is clear. Lead with a consistent application experience. Fulfil through different platforms underneath depending on the use case. Keep the account management, support and commercial relationship simple. That approach gives MSPs room to grow without multiplying effort.

Migration is still the hardest problem to solve

Despite all the talk of new technology, legacy migration remains the biggest operational challenge for many partners. There is still revenue tied up in services that are changing or disappearing. Managing that transition without damaging customer relationships or overwhelming delivery teams is difficult. What they are looking for now is not encouragement, but practical support. Clear migration paths. Automation. Commercial models that recognise the effort involved. Programmes that allow them to stabilise their base while still focusing on growth.



"Partners need to be able to focus on new business while migration happens in the background, not instead of it."
John Murphy, CEO, Gamma Business

Predictability changes the conversation

One of the most telling points in the discussion was the emphasis on predictability. Partners have long memories when it comes to missed delivery dates and slipping roadmaps. Confidence is built not by ambition, but by consistency. When a vendor can clearly say what is coming, when it is coming, and how it can be sold, the relationship changes. Planning becomes possible. Sales conversations improve. Partners can speak to customers with confidence rather than caveats.

That predictability is now a differentiator in its own right.

An external view: why this matters commercially

Matt Townend from Cavell reinforced many of these themes from an external perspective. Customers are still looking at product and price, but increasingly they are judging partners on expertise, integration capability and their ability to help navigate change. Security and compliance are no longer specialist conversations. They are baseline expectations. For MSPs with an eye on future exit, this matters even more. Platforms that are not secure or compliant will surface during due diligence. Getting it right now protects value later.

"Trust, security and route to market matter hugely when investors look at MSP businesses."
Matt Townend, Cavell

What momentum really looks like in 2026

The conclusion was not dramatic, but it was clear. The opportunity in the MSP market is real. Demand is there. Customers want more support, better experiences and smarter use of technology. But the winners in 2026 will not be the MSPs chasing every new trend. They will be the ones backing partners who reduce friction, deliver consistently, and make growth easier rather than noisier. Momentum does not come from announcements. It comes from trust, delivery and platforms that stand up to real-world pressure. **That is what MSPs care about now.**

MANAGED SERVICES SUMMIT

BENELUX
LONDON
NORDICS
MANCHESTER

CREATING VALUE with MANAGED SERVICES

managedservicessummit.com

MANAGED SERVICES SUMMIT BENELUX

benelux.managedservicessummit.com

30 JUNE 2026

MANAGED SERVICES SUMMIT LONDON

london.managedservicessummit.com

09 SEPTEMBER 2026

MANAGED SERVICES SUMMIT NORDICS

nordics.managedservicessummit.com

05 NOVEMBER 2026

MANAGED SERVICES SUMMIT MANCHESTER

manchester.managedservices summit.com

17 NOVEMBER 2026