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

THE SINGLE WAY TO MANAGE MULTI-TENANTS

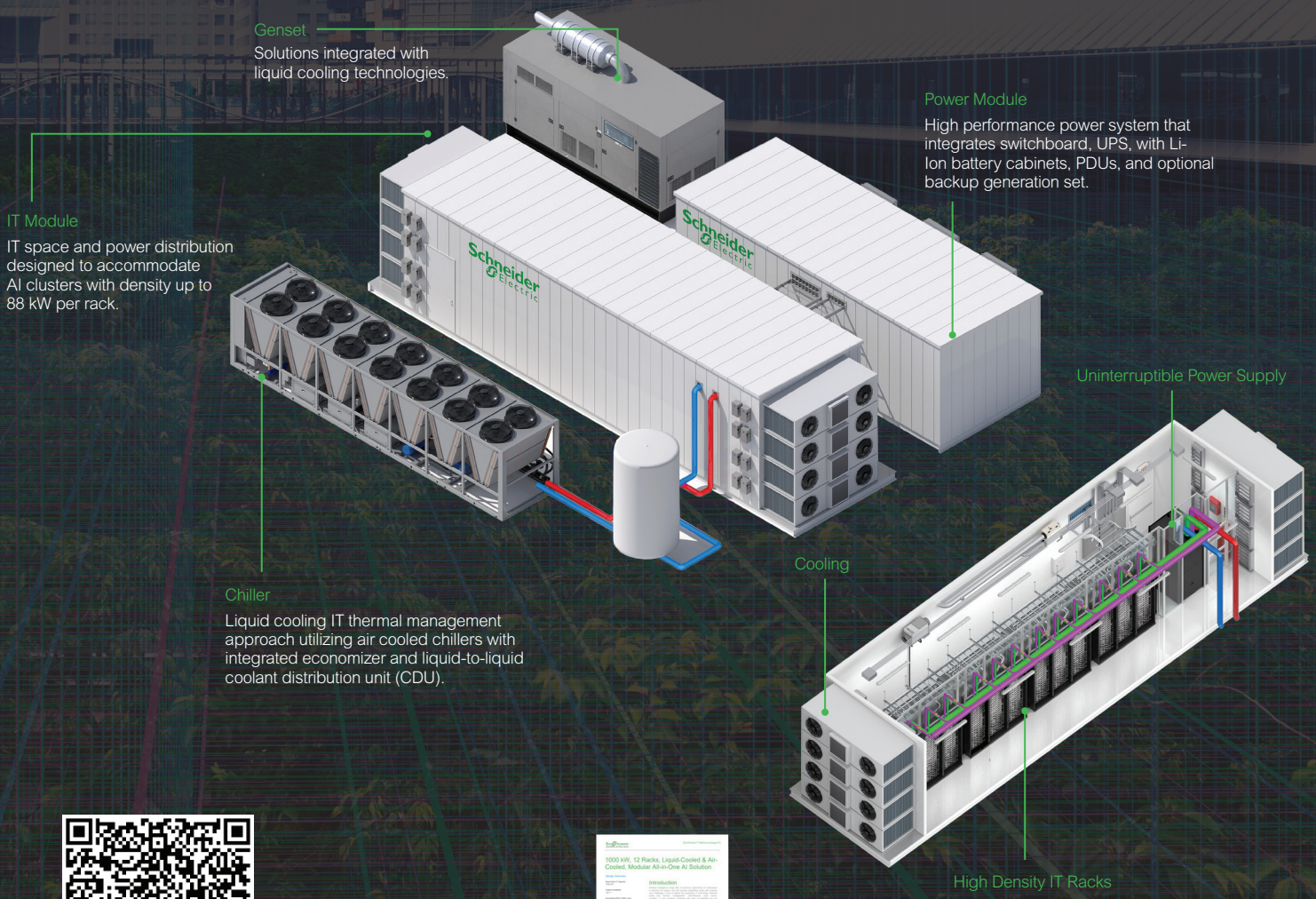
Why wait to build an AI data center when you can unpack one now!

Are you ready to revolutionize your AI infrastructure with modular data centers?

Modular AI data center from Schneider Electric present a prefabricated, scalable infrastructure solution tailored to meet the extreme power, cooling, and density demands of generative AI workloads. Discover how prefabricated modular data centers can accelerate AI adoption, simplify design and construction, and support sustainability strategies.

Download the e-guide and reference designs

to learn more how Schneider Electric's Modular AI Data Centers address these critical challenges and help you stay ahead in the evolving technological landscape!



Download the e-guide

Life Is On Schneider Electric

VIEWPOINT

BY PHIL ALSOP
EDITOR

Seizing the AI opportunity

The rise of artificial intelligence is creating a great opportunity for Managed Service Providers (MSPs), reshaping both how they deliver value and how their clients perceive their role in the digital ecosystem.

Traditionally, MSPs have been relied upon to manage infrastructure, ensure uptime, and provide security. While these services remain essential, AI offers a path for MSPs to into a position of strategic enabler, helping organisations unlock efficiency, innovation, and resilience.

At its core, AI allows MSPs to automate and enhance many of their existing services. Predictive maintenance is a clear example: rather than responding to incidents when systems fail, MSPs can leverage AI-driven analytics to identify patterns that indicate when a failure is likely to occur.

This shifts their operating model from reactive to proactive, improving service quality while reducing downtime for clients. Similarly, AI can be applied in cybersecurity to detect anomalies that may signal a breach before traditional monitoring systems would raise an alert. In these cases, the AI layer is not a replacement for MSPs, but rather a multiplier that makes their work more impactful.

Beyond improving existing operations, AI also enables MSPs to expand their service portfolios. Many small and mid-sized businesses lack the in-house expertise to deploy and manage AI themselves. This creates a natural opening for MSPs to become trusted AI partners, offering advisory, implementation, and ongoing optimization services. For instance, an MSP could help a manufacturing client deploy AI models to improve supply chain forecasting, or support a retailer in applying AI-powered personalisation to enhance customer engagement. By providing these higher-value services, MSPs move closer to the heart of their clients' strategic objectives, positioning themselves as growth partners rather than just IT caretakers.

The AI opportunity also extends inward, as MSPs can harness AI to optimise their own business models. Automating support desk operations with intelligent virtual agents reduces costs and accelerates resolution times. AI-powered business intelligence tools can help MSPs better predict client churn, identify upsell opportunities, and optimise resource allocation. This not only strengthens profitability but also enables MSPs to deliver a more tailored and anticipatory customer experience.

Ultimately, the opportunity is twofold: AI enhances the efficiency and quality of the traditional services that MSPs provide, while also opening the door to a new generation of data-driven, value-added offerings. Those MSPs who embrace AI early and develop the right expertise will find themselves in a stronger competitive position, able to differentiate in a crowded market and forge deeper, longer-lasting client relationships. In many ways, AI represents not just a technological shift for MSPs, but a chance to redefine their role in the future of digital business.

CONTENTS

ISSUE IV 2025

MSP CHANNEL INSIGHTS

The single way to manage multi-tenants

Multi-tenant management is a staple of the MSP world. A feature they 'could not live without', according to our recent survey of the industry

NEWS

MSP CHANNEL INSIGHTS

Angel BUSINESS COMMUNICATIONS

Editor
Philip Alsop
+44 (0)7786 084559
philip.alsop@angelbc.com

Senior B2B Event & Media Executive
Mark Hinds
+44 (0)2476 718971
mark.hinds@angelbc.com

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

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

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

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

Directors
Sukhi Bhadal: CEO
Scott Adams: CTO

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

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

ISSN 2396-9016 (Online)

Tool sprawl: The quiet culprit behind MSP burnout

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

A RECENT STUDY conducted by Heimdal and FutureSafe shines a spotlight on a growing issue within the Managed Service Provider (MSP) community: tool sprawl.

This phenomenon, characterised by the overwhelming number of security tools that MSPs juggle daily, is leading to operational inefficiencies, missed threats, and burnout among providers.

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

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

Unsurprisingly, all MSPs serving over 1,000 clients confessed to experiencing daily fatigue.

The study reveals that the issue extends beyond managing alerts. The fatigue resulting from disconnected platforms bore an impact on billing processes, client onboarding, and compliance. “Agent fatigue isn’t just a tech issue. It’s a business risk,” said Jason Whitehurst, CEO at FutureSafe. “MSPs are juggling tool after tool, but they don’t work together.”

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

Some of the key insights from the survey include:

- 56% of MSPs encounter alert fatigue daily or weekly, with another 75% facing it at least monthly.
- A paltry 11% benefit from seamless tool connectivity.
- MSPs relying on seven or more tools witness nearly double the levels of fatigue.
- High false positive rates increase the likelihood of missing actual incidents threefold.
- The 20% who embraced tool consolidation report favourable outcomes across all parameters.

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

AI vulnerabilities spotlighted at Pwn2Own Berlin

THE TENSION between opportunity and risk was evident at Trend’s Pwn2Own event in Berlin, where the AI category was introduced for the first time. The results offered a compelling snapshot of where AI security currently stands.

Twelve entries targeted four major AI frameworks, with the NVIDIA Triton Inference Server receiving the most attention. Chroma, Redis, and the NVIDIA Container Toolkit were also successfully exploited, in some cases using just a single bug to achieve full compromise. In total, seven unique zero-day vulnerabilities were uncovered in the AI frameworks. The vendors now have 90 days to patch the flaws before technical details are made public.

As AI becomes more deeply integrated in enterprise IT environments, Trend urges security leaders to proactively evaluate the evolving risk landscape and embed rigorous security practices into every stage of AI adoption.

Securing the future: Navigating hybrid cloud challenges

New research indicates organisations face hurdles in securing applications across diverse cloud environments, highlighting a need for unified security approaches.

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

The report, entitled "The Case for Convergence in Hybrid Multi-cloud, Application-centric Networks," reveals that an overwhelming 89% of organisations are currently using different tools and policies to secure different segments of their infrastructure. This fragmentation is complicating efforts to maintain consistent security and control across networks.

Hybrid Adoption: The study shows an

evident shift towards hybrid models, with 85% of companies engaging two or more cloud service providers, while 43% still keep applications on-premises. Many anticipate this distribution to persist long-term.

Security Siloes: Fragmentation in security tools is prominent, with nearly 80% utilising native cloud provider firewalls, alongside third-party and microsegmentation solutions. This disjointed approach compromises policy consistency and undermines visibility.

Increased Vulnerabilities: A significant 43% of the surveyed organisations reported experiencing a public cloud attack within the last two years, with prevalent issues such as malware propagation (44%), misconfigurations (32%), and open ports (26%).

Coordination Challenges: Despite some progress in integrating responsibilities for on-prem and cloud security, 55% of respondents cited insufficient collaboration among security, cloud, networking, and application teams as a key hurdle.

Operational Benefits: Beyond enhancing risk management, companies anticipate significant operational benefits from improved network security. The research highlights increased efficiency (63%), reduced costs (48%), and expedited cloud migrations (46%) as top advantages.

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

Widespread AI adoption in cybersecurity strategies, but mounting concerns over cyber risk exposure

TREND MICRO has published research revealing that while organisations are embracing artificial intelligence to strengthen cyber defences, many are increasingly concerned about the technology's potential to expand their attack surface and introduce new risks.

Rachel Jin, Chief Enterprise Platform Officer at Trend Micro: "AI holds enormous promise for strengthening cyber defences, from identifying anomalies faster to automating time-consuming tasks. But attackers are just as eager to leverage AI for their own purposes, and that creates a rapidly shifting threat landscape. Our research and real-world testing make it clear that security must be built into AI systems from the outset. There is simply too much at stake to treat this as an afterthought."

According to the study, 81% of global businesses are already using AI-driven tools as part of their cybersecurity strategy, with this number rising to 86% for UK businesses. Nearly all global respondents (97%) are open to using AI in some capacity. Over half are already relying on it for essential processes such as automated asset discovery, risk prioritisation and anomaly detection. AI and automation are now considered top priorities for improving cybersecurity over the next 12 months by 42% of surveyed organisations.

This optimism also comes with significant risk. An overwhelming 94% of global businesses believe that AI will negatively impact their cyber risk exposure within the next three to five years. 66% of UK businesses flag worries that AI-driven attacks will drastically increase in complexity and scale over this period. UK businesses call out increased risk of AI-powered phishing or social engineering attacks (54%), exposure of sensitive (41%) and proliferation of shadow IT (38%) most often when pointing to their AI security risks of most concern.

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

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

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

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

Despite this optimism, the data suggests that much of this confidence could be superficial. In the UK, 44% of IT leaders spend a quarter of their working month resolving critical issues and service disruptions.

Alarmingly, nearly a third (32%) report spending even more time, with an unlucky few saying up to 90% of their

month is consumed by such problems. This highlights a clear disconnect between perceived confidence and the day-to-day reality of managing IT disruptions.

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

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

Despite these hurdles, UK IT teams are taking a proactive approach and investing heavily in operational resilience. The majority (63%) report that up to 30% of their IT budget is now devoted to disruption prevention. Across Europe, more than two thirds (69%) are upgrading tools, training and playbooks to improve internal recovery and response processes for when disruptions occur.

Transformative AI trends in the vCISO landscape

CYNOMI, a distinguished vCISO platform provider for Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs), has unveiled the company's latest findings in its 2025 State of the vCISO Report.

This comprehensive analysis highlights AI's transformative impact on cybersecurity and compliance management, spotlighting vCISO services as a burgeoning growth area.

The data demonstrates a substantial upward trajectory, with the percentage of managed service providers offering vCISO services surging from 21% to 67% year-over-year. As market demand intensifies, providers are leveraging AI as a strategic tool to deliver sophisticated services more profitably with reduced resource investment.

Key findings include:

- AI is already realising significant time efficiencies, with an average 68% reduction in vCISO workflow burdens.
- 81% of vCISO service providers are already incorporating AI and automation in their practices, with another 15% intending to do so within the next year.
- Estimates suggest AI could diminish labour time by 58% across cybersecurity and compliance service executions.

Despite these advancements, challenges exist, such as high initial costs, a shortage of skilled personnel, and the volume of time-consuming tasks. Here, AI-powered platforms present viable solutions by cutting labour hours and streamlining complex issues in cybersecurity and compliance domains.

Cynomi's platform, designed to enable this evolution, facilitates MSPs and MSSPs in delivering vCISO services with enhanced speed and efficiency. Features include automated risk assessments and compliance readiness, reducing manual workloads by up to 70%, thereby enhancing profitability, prolonging customer lifetime value, and securing a competitive advantage.

Industry gap in operationalising threat intelligence

Cyware has released new research revealing that a majority see the importance of having a Threat Intelligence Program and have started a Program.

HOWEVER, 80% of respondents recognise their threat intelligence programs are not fully operationalised, highlighting a significant opportunity for threat intelligence automation.

The findings, gathered from security professionals at InfoSec Europe 2025, expose critical gaps in the maturity and automation of legacy threat intelligence platform capabilities, as well as a growing appetite for AI-driven solutions to augment speed, context and actioning of threat intel.

Further survey results support this gap in operationalised threat intelligence, where 30% noted they are grappling with too many feeds with too little context, followed by a lack of automation/playbooks capabilities at 29%, and insufficient dedicated staff at 18%.

All of these challenges reflect the need for maturing and operationalising threat intelligence that can be addressed with an AI-driven, automation-rich threat intelligence platform (TIP).

Survey responses identified the most in-demand TIP capabilities as follows: automation (48%), contextualisation and enrichment (37%) and more accurate risk scoring (34%). “We are excited to see this validation, coming straight from security practitioners, for how we’ve designed automation across the threat intelligence management lifecycle,” said Anuj Goel, CEO and Co-founder of Cyware.

“Our unified threat intelligence solution automates ingestion, normalisation, de-duplication, enrichment and all the way through to threat actioning, facilitating and accelerating the full threat workflow.”

The automation theme continued in survey results, with over half (51%) of

cybersecurity professionals believing AI is best placed to automate triaging and prioritisation of threats. Cautious excitement exists with AI, where 61% said they would only trust AI agents to take limited autonomous actions (such as blocking IOCs or quarantining endpoints) provided there was still human oversight.

“The survey confirms what many in the industry are already feeling – that traditional approaches to threat intelligence are no longer enough,” said Brett Candon, VP International at Cyware. “Security teams need AI-powered tools that can enrich data with context, automate time-consuming workflows and support real-time decision making. The opportunity is an augmented system from AI and automation that maintains human verification or oversight while improving their capacity to defend against the volume and complexity of today’s threats.”

Additional key research findings include:

- Only 20% of respondents said they are “fully operationalised” in their use of threat intelligence with response integration–reflecting the gap in legacy TIP with current threat intelligence program requirements.
- Of those using a legacy TIP, only 17% use it to automate response workflows and 27% to enrich incidents and alerts–exposing untapped potential in modern TIPs.
- Only 16% of TIP users are currently sharing intelligence with partners or peers, despite nearly 75% recognising a need to improve sharing practices–further identifying opportunities with modern TIP capabilities.
- Only 38% of organisations have a defined threat intel sharing process that includes their supply chain, suggesting a missed opportunity for building greater resilience through collaboration.
- 39% identified AI-assisted correlation of IOCs and TTPs as the most valuable capability in an AI-powered TIP.

The survey confirms what many in the industry are already feeling – that traditional approaches to threat intelligence are no longer enough

UK businesses face major revenue losses due to network instabilities

Network disruptions cost UK businesses millions, prompting renewed focus on connectivity and related IT investments.

NETWORK instability has emerged as a significant challenge for UK businesses, with a third (33%) reporting revenue losses of up to £4 million due to outages or poor performance.

Alarmingly, another 18% have experienced losses exceeding £4 million, according to a study by IDC InfoBrief, commissioned by Expereo. The report, titled "Enterprise Horizons 2025: Technology Leaders Priorities: Achieving Digital Agility," highlights the pervasive impact of recent IT disruptions.

Following cybersecurity breaches and connectivity failures, half of UK businesses have reconsidered their technology infrastructure, with 35% noting an increase in the importance of networking and connectivity in executive discussions.

Networking/connectivity now leads in

terms of financial investment priorities for UK businesses over the next year (40%), surpassing cybersecurity (39%) and AI (35%). This marks a shift from last year when AI topped the list and networking/connectivity came third, showcasing a recalibration of priorities to address immediate networking concerns.

The urgency is palpable. Over 27% of UK organizations claim inadequate network performance threatens growth plans, while almost half (49%) acknowledge network limitations impede their data and AI initiatives. Notably, a mere 5% of businesses are confident their networks can fully support AI endeavors without obstacles.

"To drive a sustainable competitive advantage, connectivity is no longer an IT concern – it's a strategic business imperative," said Ben Elms, CEO of Expereo. "...As businesses race to adopt new AI solutions, the C-suite must treat network performance with the same urgency as cybersecurity and AI itself..."

Beyond infrastructure, talent acquisition remains a critical challenge. Cybersecurity tops the list of areas where finding skilled professionals is difficult (44%), closely followed by networking (40%). Consequently, 40% of UK businesses are increasing reliance on external partners, such as vendors or managed service providers, to address networking skill shortages.

New research highlights MSPs' growing role in cybersecurity landscape

BARRACUDA NETWORKS, INC., a leader in cybersecurity solutions, has unveiled the MSP Customer Insight Report 2025, shedding light on the growing significance of Managed Service Providers (MSPs) in enhancing cybersecurity for businesses globally.

Commissioned by Barracuda and executed with Vanson Bourne, the survey spanned 2,000 IT and security decision-makers across the Americas, Europe, and Asia-Pacific. Findings reveal an urgent demand for MSPs and their advanced security solutions among businesses of all sizes.

- **MSPs are pivotal for growth:** Over half (52%) of surveyed businesses count on MSPs to manage the increasing number of disparate security tools, while 51% expect assistance in evolving security strategies amid business growth. Nearly half (48%) seek 24/7 security coverage from MSPs, highlighting their indispensability.
- **High MSP collaboration rates:** About 73% of businesses already partner with MSPs, with the number soaring to 96% when including those considering such partnerships.
- **Expanding client base:** While traditionally catering to smaller firms, MSP reliance spans to 85% of larger organizations (1,000-2,000 employees) versus 61% for smaller counterparts (50-100 employees).
- **A future focus on AI and Zero Trust:** Emerging technologies like AI and machine learning are expected to drive MSP demand, alongside modern security protocols such as Zero Trust and managed security operations.
- **Premium services demand premium pay:** A notable 92% of businesses are willing to spend up to 25% more on MSP services, emphasizing MSPs' crucial role in cybersecurity.

However, customer expectations are equally high. Businesses are willing to switch MSPs if they fall short in recovery from cyberattacks or fail to evidence robust 24/7 security expertise, with 45% indicating a readiness to change providers under such circumstances.

Navigating hybrid cloud challenges

New research indicates organisations face hurdles in securing applications across diverse cloud environments, highlighting a need for unified security approaches.

A NEW STUDY conducted by the Enterprise Strategy Group (ESG) has highlighted the increasing challenges organisations face in securing applications within hybrid cloud environments.

Commissioned by cybersecurity leader AlgoSec, the research points to the growing inadequacy of traditional network security strategies as applications become dispersed across on-premises data centres and various cloud platforms.

The report, entitled "The Case for Convergence in Hybrid Multi-cloud, Application-centric Networks," reveals that an overwhelming 89% of organisations are currently using different tools and policies to secure different segments of their infrastructure.

This fragmentation is complicating efforts to maintain consistent security and control across networks.

- **Hybrid Adoption:** The study shows an evident shift towards hybrid models, with 85% of companies engaging two or more cloud service providers, while 43% still keep applications on-premises. Many anticipate this distribution to persist long-term.
- **Security Siloes:** Fragmentation in security tools is prominent, with nearly 80% utilising native cloud provider firewalls, alongside third-party and microsegmentation solutions. This disjointed approach compromises policy consistency and undermines visibility.
- **Increased Vulnerabilities:** A significant 43% of the surveyed organisations reported experiencing a public cloud attack within the last two years, with prevalent issues such as malware propagation (44%), misconfigurations (32%), and open ports (26%).
- **Coordination Challenges:** Despite some progress in integrating responsibilities for on-prem and cloud security, 55% of respondents cited insufficient collaboration among security, cloud, networking, and application teams as a key hurdle.
- **Operational Benefits:** Beyond enhancing risk management, companies anticipate significant operational benefits from improved network security. The research highlights increased efficiency (63%), reduced costs (48%), and expedited cloud migrations (46%) as top advantages.

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

AI adoption, risk assessments, and leadership alignment drive security maturity

Vanta has released its Trust Maturity Report, offering a data-driven look at how organizations are evolving their security programs in an increasingly complex risk landscape.

Drawing on aggregated, anonymized insights from over 11,000 organizations and aligned to the NIST Cybersecurity Framework (CSF), the report maps companies across four security maturity tiers:

- **Partial –** Organizations in the earliest stage of maturity, typically relying on limited or ad hoc security processes
- Risk-Informed – Teams that have begun to formalize risk management practices, though application is often inconsistent
- **Repeatable –** Companies with standardized, organization-wide security practices that are actively maintained
- **Adaptive –** Highly mature organizations that continuously optimize and scale their security programs through automation, analytics, and cross-functional alignment.

As organizations progress through these tiers, the report shows a clear pattern: higher maturity correlates with better risk practices, stronger resilience and more effective use of AI.

Key findings from the report reveal:

- **Risk assessments are a turning point:** Only 43% of Partial companies have completed a risk assessment, compared to 100% for Adaptive
- **Budget remains a barrier at all stages:** 67% of Repeatable and 35% of Adaptive companies cite budget and resources as ongoing challenges
- **Incident preparedness signals maturity:** 92% of Repeatable companies monitor threats continuously with alerts compared to 56% of Partial companies with a basic incident response plan that's not tested, and 12% with no plan at all
- **AI drives scale and efficiency at the top:** 71% of Adaptive companies are adopting AI to enhance speed, scale, and efficiency.

"Security maturity doesn't happen by accident—it's driven by deliberate, strategic investment in risk management, culture and ongoing incremental improvements to people, process, and technology," said Jadee Hanson, CISO, Vanta. "Our data shows that organizations that embed trust principles in everything they do mature faster, operate more resiliently, and are better prepared for today's evolving risk landscape."

Security maturity starts with strategic risk management

One of the clearest markers of maturity that divided the Partial from the other, more advanced tiers is risk assessments. Vanta's research found that only 43% of Partial organizations conduct risk assessments, while 100% of Risk-Informed businesses have conducted at least one formal risk assessment. This shows how external factors like compliance requirements and customer needs are often the biggest drivers of early-stage security programs.

Incident readiness was also a clear indicator for maturity. Vanta found that 92% of those at the advanced tiers (Repeatable & Adaptive) monitor threats continuously with alerts. Specifically, for Repeatable organizations:

- 100% have business continuity plans
- 85% run regular incident response drills
- 78% test their plans regularly

AI is a key enabler for mature security teams

Adaptive companies are significantly more likely to adopt and integrate AI into their security operations. With a better understanding of their data flows, governance needs and risk exposure, these organizations use AI to reduce rework, streamline decision-making and align with frameworks like ISO 42001.

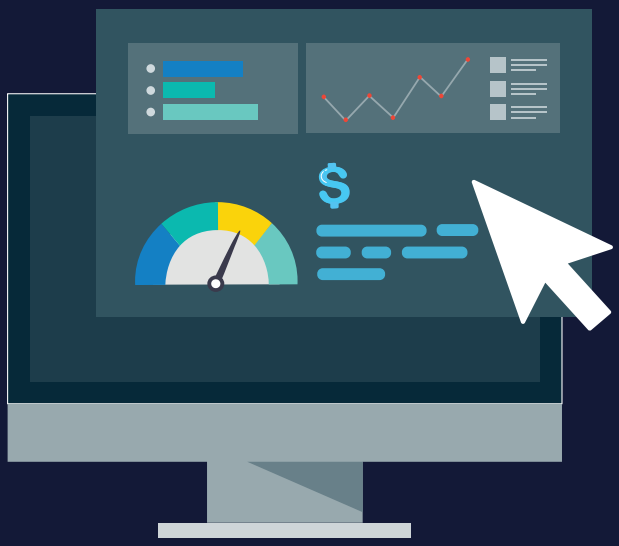
Trust-first teams drive maturity

Trust isn't just a byproduct of mature security programs; it's what drives them forward. As organizations progress, they embed trust into company culture, secure leadership alignment and integrate risk into top-level decision-making. For Partial organizations, security investments are largely driven by customer expectations and compliance needs. For Adaptive, the top drivers are responding to customer/vendor demands (95%), reducing security risks (93%), meeting compliance requirements (90%), scaling security operations (75%), differentiating through security maturity (70%) and managing multiple frameworks (35%).

datto
A Kaseya COMPANY

Boost MSP Productivity & Profitablity with Datto BCDR

Reduce downtime, streamline operations & grow recurring revenue.



LEARN MORE

www.datto.com/partner-request/bcdr

The single way to manage multi-tenants

Multi-tenant management is a staple of the MSP world. A feature they 'could not live without', according to our recent survey of the industry.

BY TROELS RASMUSSEN, GM OF SECURITY, N-ABLE.

THESE TOOLS allow vendors to scale operations and onboard new customers without putting additional strain on the team. While multi-tasking is something MSPs are familiar with, the act of juggling multiple clients without a single interface opens the door to security threats, reduces efficiencies and drains resources. Instead, MSPs should invest in a trusted tool that allows them to scale activities across clients and reduce the risk of human error.

It's easy to see why these tools are necessary, but they are not all created equal. Selecting the right one will support current and future business goals while enabling effective resource management. To make the selection process simpler, I've outlined why multi-tenant management is essential and provided the five steps to choosing the right tool. This includes matching the tool with the needs of the business, making sure employees have the correct training and partnering to fill any gaps.

Why multi-tenant management should be a business staple

For MSPs, multi-tenancy isn't optional; it's an essential part of seamlessly managing clients. From an operational perspective, it's much simpler and cost-effective to manage multiple customer environments from a single interface without manually switching between them. Processes such as onboarding new customers can be simplified and automated to free up time for MSPs. This allows them to focus on core responsibilities and delivering value, without needing additional team members.

Having a single view also positively impacts compliance as policies can be applied across tenants seamlessly. Remaining compliant is one of the keys to true resilience and this method of keeping data secure and encrypted ensures that customers remain in line with global data protection laws.

The business impact of choosing the right tool

Our recent Horizons report highlighted the importance of these tools, with one MSP commenting, "Everything I buy is multi-tenant. I want to see all the backups, cameras, Azure virtual machines and I want to control them from one point and be in control financially and operationally."

For businesses trying to scale and onboard new customers, especially if they are targeting larger business, choosing the wrong tool can be very limiting. The Consortium of Information & Software Quality estimated that poor software quality cost US businesses $2.41 trillion in 2022. While not directly related to multi-tenant management, it does show how choosing the wrong tool can get expensive. It's clear that selecting the right platform is essential for sustained growth and secure client management, ultimately increasing customer retention and trust.

Multi-tenancy is the standard for MSP tools, and it won't be long before AI-powered multi-tenant management becomes the new standard.

Expert insight: Five-steps to picking the winner

1. Match the tool to business needs
Take the time to understand your current operations and remember that these tools will need to evolve as your business grows. It's worth mapping out future growth plans, including the number of tenants you might need to support, and combining these with the priorities you have set out. This will act as a useful filter when evaluating features of specific tools against operational needs. For example, automation, security policy enforcement, storage requirements and scalability.

2. Ensuring a personalised experience for tenants
While it's important to manage

tenants from a single interface that doesn't mean each tenant has the same requirements. Their experience must still be personalised. There also shouldn't be any crossover of data between tenants, in keeping with regulatory requirements.

As mentioned, compliance is critical to resilience which further exemplifies the need for tenant isolation. Customisation per tenant is the key to managing these differing requirements.

3. Cost of running the tool
Cost is always a factor in the selection process. It's critical to consider the resources that will need to be allocated to each tenant via different models including database, compute and storage. This will inform conversations around the operational costs and benefits of each model which will likely result in an intelligent outcome.

4. Operational complexity
It's important to establish standard operating procedures to help set the baseline and generate guidelines for managing tenants, onboarding, and configuration. Therefore, a key factor when considering what to buy is operational complexity, particularly looking at how performance will be monitored and managed across tenants.

This is the same for databases, with factors to consider such as back-up and restoration processes.

5. Identify gaps and partner strategically to fill them
This is the time to make outsourcing versus internal development decisions. Partnering with vendors can enable access to specific certifications and support necessary to optimise the use of their tools. Regulations are another area where partners can add value. Depending on the country and sector being served, you should audit the regulatory requirements across your business and clients to find what's missing. Armed with this information, you can make better partner selection decisions.

Once the tool is implemented, the next step is to prioritise staff training. Ensuring internal teams are properly onboarded to the tool will make its operation and use much smoother. Continuous training will keep staff ahead of any new or updated features to top up this base-knowledge. And finally, set up continuous monitoring and alerting which will help to detect and respond to security threats in real-time.

All MSPs, and particularly those looking to grow their customers base or target larger customers, need multi-tenancy. And most importantly, the right tool for them. We often talk about the administrative tasks burning through the valuable time of an MSPs team and moving to a single interface for tenant management is one of the solutions to alleviate this pressure while also increasing efficiency and security.

Following the five-steps covers all bases from scalability and security to finding the right partner to work with. Choose wisely, train thoroughly, and partner smartly to grow and ultimately, stay secure.

For businesses trying to scale and onboard new customers, especially if they are targeting larger business, choosing the wrong tool can be very limiting. The Consortium of Information & Software Quality estimated that poor software quality cost US businesses $2.41 trillion in 2022

Unlock the power of Teams in a modern workplace

Workplace collaboration is being reshaped by the evolving modern workplace, fuelled by technological advancements and the rise of soft interfaces and unified communications (UC) tools like Microsoft Teams. Its adoption is at an all-time high and still rising, quickly becoming the default communication platform for businesses with over 320 million monthly active users worldwide.

BY MYLES LEACH, MANAGING DIRECTOR NFON

YET WHILE the move to digital collaboration has been revolutionary, Microsoft Teams lacks basic critical service many businesses need – integrated enterprise-grade voice and customer service solutions. With the global Unified Communications as a Service (UCaaS) market set to grow to over 131 million users by the end of 2028 at over 10.3% growth per year, MSPs have an opportunity to meet this demand by adding on voice solutions and gain entry into a new market by offering solutions that integrate with Teams.

Balancing voice with modern tools

Voice communication is an irreplaceable mode of connection that just simply can't be replaced by chat alone. Now, businesses can leverage integrations to unify their existing voice services within Microsoft Teams, creating a seamless hub for collaboration, chat and calling.

The result is that employees would no longer have to juggle between different tools to communicate effectively. They can now consolidate all forms of communication to enhance both internal collaboration and client interactions.

The lack of a voice integration in Microsoft Teams represents a huge new opportunity for resellers and MSPs. According to our recent research into MSP opportunities in the UK, no respondents from organisations of under ten employees had a UC solution in place. Yet despite this, nearly half (48%) of MSPs have not decided to introduce a communications solution or are still undecided about it.

This is a missed revenue stream that MSPs can tap into as having an UCaaS solution brings on many benefits and makes for a much more compelling value proposition. MSPs benefit from higher recurring revenue because MSPs can move beyond the one-off Microsoft license sales. MSPs also benefit from increased customer retention because the more critical services MSPs provide the sticker they become to customers. Customers, in turn, experience reduced vendor fragmentation and a more streamlined communication experience.

Building for the future

The future of customer engagement with Microsoft Teams is heading toward a more integrated, AI-driven experience that enhances personalisation and

efficiency. Improving customer experience and enhancing hybrid work collaboration top the list of reasons for why customers are adopting new communications solutions. Therefore, as AI tools within Teams continue to evolve, we can expect businesses will want more advanced features for tracking customer engagement, sentiment, automating routine interactions, and providing instant insights to improve service quality.

Integrations with CRM and productivity tools are likely to deepen too, making it easier for businesses to access and leverage customer data in real-time during interactions, creating a seamless customer experience. Virtual meetings will also drive demand for more immersive, interactive communication formats, where features like real-time transcription, language translation, and enriched collaboration spaces become standard.

As Teams becomes a full-service customer engagement platform, MSPs should stay alert to the need to offer new integrations for AI capabilities, in order to remain competitive and responsive to customer needs.

The way forward

Although this trend presents significant opportunities for MSPs, introducing new solutions can come with its own challenges that can get in the way of financial, competitive, and operational benefits. Our research shows that the lack of in-house expertise, sales knowledge and concerns about cost

were some of the most pressing challenges MSPs have in taking unified communication solutions to market.

The variety of concerns we've heard voiced by MSPs across the sector clearly indicates which vendors are best positioned to give support. For MSPs aiming to meet growing customer demand for voice solutions, selecting a vendor that meets both current and future needs will help them fully integrate solutions without complex infrastructure investments. Therefore, vendors with well-structured and comprehensive Partner Programmes are best placed to address the concerns that vendors have and to meet future customer demand.

Embracing the evolving landscape

Microsoft Teams has been a fundamental shift in how businesses communicate and collaborate. However, critical voice and contact centre solutions have been left behind to some extent in the digital collaboration movement, leaving smaller businesses at a distinct disadvantage.

MSPs can help place that final piece in business collaboration and introduce a new generation of voice integrations to Teams that are more accessible to businesses to all sizes and are designed to scale seamlessly as Teams heads towards more AI-driven experiences. The MSPs who seize the opportunity will unlock a new market, solidify their customer relationships and establish themselves as key players in the future of workplace communication.

Securing the future: Why IT and security can't afford to operate in siloes

In the past, IT and security teams operated in siloes, only collaborating or exchanging information when it was absolutely necessary. However, the rise of the cloud and remote work caused those traditional siloes to blur. Organisations had to ensure that employees had both the technology and IT support to work where and how they wanted, and that they were also secure in doing so.

BY MIKE ARROWSMITH, CHIEF TRUST OFFICER, NINJAONE

NOW, thanks to 'endpoint sprawl' (the rapid adoption of diverse devices and operating systems across environments), BYOD, and a widening threat landscape, organisations find themselves contending with a new variety of heightened risks.

Up against a rapidly evolving world, divided IT and security teams aren't just ineffective, they're unsustainable. It's no longer just a nice-to-have for IT and security teams to work together to boost productivity while reducing risk; it's vitally important for organisations and businesses to succeed in our hyperconnected digital world. For organisations still struggling to streamline better IT/security collaboration or hoping to get a better understanding of what it looks like in practice, here are a few important themes to consider.

Shared talent will lead to better IT-security alignment

As economic uncertainties continue and the IT skills gap widens, stronger IT-security alignment isn't just better for business; it's a more effective use of the current talent pool. As Tech UK notes, businesses are increasingly looking for professionals who possess both IT and security skills to fill technical roles.

Technical incidents which can often arise from poorly managed endpoints (think: a remote employee inadvertently clicking on a phishing email that takes down the whole organisation), underscore this growing overlap. As more cyberattacks originate at the endpoint, we're seeing more often that the same people responsible for managing those endpoints are the ones

MSP CHANNEL AWARDS 2025

CELEBRATING 15 YEARS OF SUCCESS

WE'RE PROUD TO HAVE LAUNCHED THE MSP CHANNEL AWARDS

INTRODUCING THE MSP CHANNEL AWARDS

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

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

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

NOMINATIONS ARE NOW OPEN

KEY DATES:

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

* Voting will close 17:30 GMT

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

NOMINATE NOW!

mspchannelawards.com

T: +44(0)2476 718 970

Angel BUSINESS COMMUNICATIONS

SDC AWARDS

ANGEL EVENTS

being tasked with investigating security breaches and forensics when they occur, making cross-functional expertise critical. Understanding whether an issue came from an unmanaged device, a vulnerable vendor, or a larger security flaw, and then quickly solving for the problem, is essential to diagnose and resolve threats before they can impact business.

More versatile talent doesn't just mean a more effective business. It also makes for greater growth opportunities for employees. As the threat landscape evolves, security awareness and education across an organisation will play a growing role in building resilience.

Consolidating tools

Bringing IT and security teams closer together isn't just about focusing on shared skill sets. It's also about empowering both teams with the tools they need to naturally bridge that gap. With shared visibility through more integrated platforms, both teams can gain real-time insights into infrastructure status, threats, and vulnerabilities. These solutions help IT and security teams rapidly exchange critical information, accelerating their response to incidents and reducing the chance of errors or misunderstandings.

Centralised and automated tools can further reduce manual effort, allowing both teams to concentrate on big-picture objectives instead of spending hours on routine tasks like patching, scanning, and incident triage.

Enhanced analytics and reporting capabilities, and tailored recommendations can lead to even deeper insights, better decision-making, and improved performance across both teams as well.

By leveraging platforms with an emphasis on unified visibility, automation, and documentation, organisations can foster greater alignment on priorities and shared accountability, leading to more agile and proactive IT and security outcomes, while strengthening organisational resilience, improving efficiency, and boosting employee productivity.

Improved collaboration, improved resilience

While we've been talking about greater IT and security collaboration for years now – and it's exciting to see the strides we've made in having those two teams collaborate better across the board – there's never been a more apt time for IT and security to work in tandem. The AI-enabled threat landscape is drastically widening organisations' digital attack surface, and we're still just seeing the tip of the iceberg.

As organisations grow, adding new employees, customers, and digital resources to their rolodex, so too does their risk. Where greater IT/security alignment will be even more essential for boosting organisational productivity in this AI-era (as more AI-enabled tools and resources and introduced to the workforce, and as employees continue to operate from anywhere), misalignment will only lead to greater chaos – introducing a plethora of new risks while potentially leading to larger conflicts when it comes to employee productivity, business efficiency, and employee enablement.

In the technical world, the ground is always moving, and organisations should continue to invest in deep collaboration between IT and security teams to enable secure innovation while scaling business. Ultimately, businesses that focus on shared skillsets, clear communication, aligned leadership, and integrated technology solutions will be the ones best positioned to strengthen their cyber resilience while achieving a competitive edge.

Technical incidents which can often arise from poorly managed endpoints (think: a remote employee inadvertently clicking on a phishing email that takes down the whole organisation), underscore this growing overlap. As more cyberattacks originate at the endpoint, we're seeing more often that the same people responsible for managing those endpoints are the ones being tasked with investigating security breaches and forensics when they occur, making cross-functional expertise critical

MANAGED SERVICES SUMMIT LONDON

10.09.2025

CONVENE
155 BISHOPSGATE LONDON

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

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

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

INDUSTRY INSIGHTS

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

BREAKOUT SESSIONS

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

NETWORKING OPPORTUNITIES

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

INTERACTIVE EXPERIENCES

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Angel BUSINESS COMMUNICATIONS

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

IT EUROPA

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

https://london.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS IT EUROPA ANGEL EVENTS

Why MSPs hold the key to infrastructure success and growth

Why MSPs hold the key to infrastructure success and growth

BY PAUL SPECIALE, CHIEF MARKETING OFFICER, SCALITY

In the 2020s we've crossed a Rubicon in the AI revolution. What were once long-discussed concepts about the possibilities and pitfalls of AI have exploded into reality. With generative tools leading breakthroughs in content creation, data analysis, and coding, the market reflects this momentum - AI is set to soar from $93 billion in 2020 to $826 billion by 2030.

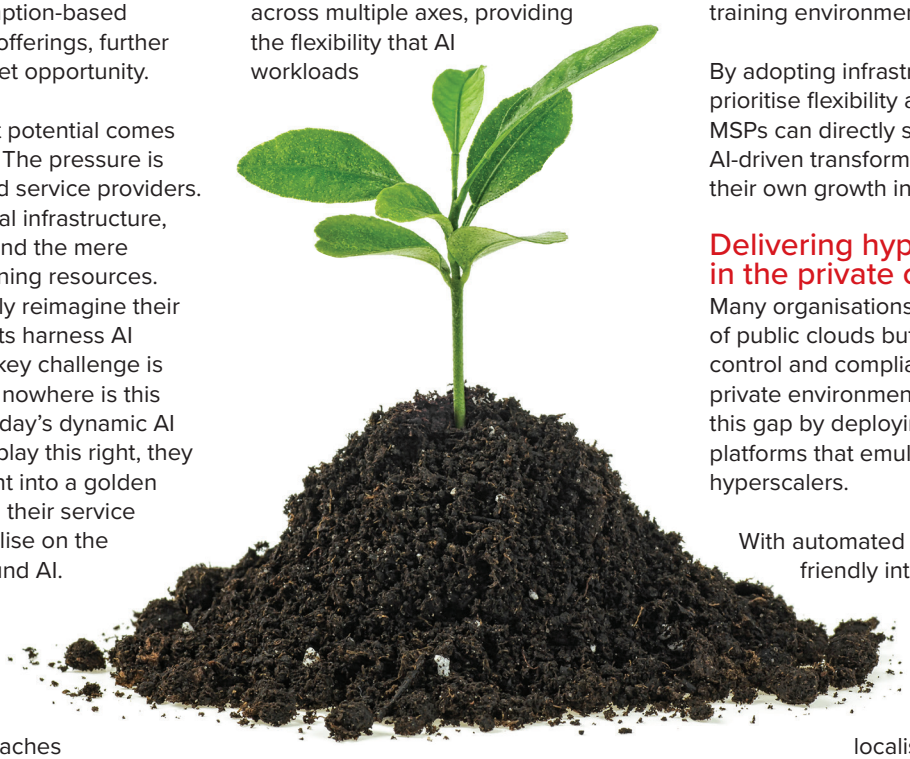
Moreover, key analysts like Gartner now predict a massive growth in enterprise demand for consumption-based as-a-service based offerings, further amplifying the market opportunity.

However, with great potential comes great responsibility. The pressure is now on for managed service providers. As stewards of digital infrastructure, MSPs must go beyond the mere baseline of provisioning resources. They need to entirely reimagine their role in helping clients harness AI effectively. But this key challenge is also a chance - and nowhere is this more true than in today's dynamic AI landscape. If MSPs play this right, they can turn this moment into a golden opportunity, expand their service offerings and capitalise on the growing needs around AI.

Legacy storage is tired

Traditional infrastructure approaches - especially legacy storage systems - are now totally inadequate for today's demands. They are not designed to handle the unpredictable, dynamic, high-throughput demands of AI workloads.

To remain relevant and create long-term value, MSPs should therefore opt for super-agile, software-defined, multidimensional scaling solutions. This approach empowers them to scale infrastructure independently across multiple axes, providing the flexibility that AI workloads demand. As AI reshapes industry expectations, clients want partners who understand the strategic value of AI and can architect infrastructure that accelerates innovation. To step into this expanded role, MSPs must evolve from service providers into strategic AI advisors. This means investing in a highly flexible, scalable, intelligent infrastructure that aligns with business outcomes - whether enabling real-time analytics, streamlining data governance, or scaling AI model training environments.



By adopting infrastructure models that prioritise flexibility and performance, MSPs can directly support their clients' AI-driven transformations and secure their own growth in the process.

Delivering hyperscaler agility in the private cloud

Many organisations seek the elasticity of public clouds but require the data control and compliance guarantees of private environments. MSPs can bridge this gap by deploying private cloud platforms that emulate the agility of hyperscalers.

With automated scaling, user-friendly interfaces, and rapid provisioning, MSPs can meet client expectations while ensuring data remains secure and localised.

Packaging scale with compliance as a unified offering

AI workloads are inherently unpredictable, with spikes in data usage and performance needs. Through multidimensional scaling, MSPs can fine-tune their infrastructure - ramping up resources only where needed.

This not only prevents overprovisioning but also ensures that sensitive data remains compliant with industry regulations, such as GDPR or HIPAA.

Going local: optimising infrastructure for data sovereignty

As data privacy regulations tighten globally, localised infrastructure is becoming a necessity. By deploying regional cloud offerings,

MSPs can help clients meet national data residency requirements while delivering low-latency performance. This localised approach is not just a compliance measure - it's a strategic advantage.

Supporting consumption-based and multi-tenant models

The shift to AI is accelerating the demand for flexible billing models. MSPs should offer consumption-based pricing and multi-tenant architecture to accommodate the bursty, iterative nature of AI development. This ensures clients can scale up or down based on actual usage, improving satisfaction while maintaining cost transparency.

MSPs that proactively support AI workloads with tailored infrastructure are positioned to unlock significant new revenue streams. AI is resource-intensive, and clients are seeking partners who can meet these requirements with resilient, high-performance solutions.

AI infrastructure spend

The demand for compute and storage is rising in tandem with AI adoption. MSPs that offer AI-optimised SLAs, scalable capacity, and high-throughput processing will stand out as preferred partners in this growing market.

With multidimensional scaling, MSPs can deliver infrastructure that precisely matches workload demands. Whether scaling up storage for massive datasets or reducing latency for inference workloads, this tailored approach boosts efficiency and protects margins - turning infrastructure from a cost center into a strategic asset.

Now is the time to embrace modern storage offerings

The age of AI demands a new playbook for infrastructure - and MSPs have a pivotal role to play. By embracing software-defined, multidimensional storage scaling, MSPs can provide the flexibility, performance, and compliance clients need to succeed in a data-driven world. This transformation isn't just about technology—for MSPs, it's a golden growth strategy. Those who act now will be better positioned to serve AI-driven businesses, open up new revenue channels, and evolve into indispensable partners in digital innovation. MSPs that welcome the challenges of AI today will lead the market tomorrow.

The global regulatory convergence:
a catalyst for smarter compliance

The convergence of global regulations shouldn't be seen as a challenge to overcome but as a catalyst for smarter, stronger, and more sustainable enterprise operations.

BY SEAN TILLEY, SENIOR DIRECTOR SALES OF EMEA AT 11:11 SYSTEMS

AS DIGITAL technologies and threats transcend borders, the global convergence of regulatory frameworks is no coincidence. Governments and regulators are recognising the need for consistency as cyberattacks, data breaches, algorithmic bias, and systemic failures in digital infrastructure are no longer local concerns but are global risks that require harmonised solutions.

This is evident in the development of regulations such as the European Union's General Data Protection Regulation (GDPR), the Digital Operational Resilience Act (DORA), the Artificial Intelligence Act, and cybersecurity rules like NIS2. With other regions adopting similar principles of transparency, accountability, and resilience.

For companies operating internationally, convergence involves transitioning from a diverse set of local regulations to a unified compliance standard.

Implications for businesses

Working as a cross-border business opens organisations up to the complexity of navigating the matrix of overlapping laws and stricter regulatory standards, whilst also managing the geopolitical tensions that can amplify both the threat environment and regulatory scrutiny.

Regulators now require faster breach notifications, formal impact assessments for high-risk AI systems, and stricter controls over third-party vendors. This includes:

- **Faster Incident Reporting:** Regulators now demand breach notifications within tight windows. For example, under GDPR, you must notify your lead data-protection authority within 72 hours of discovering a personal data breach before deploying a credit-scoring AI model.
- **Formal Risk/Impact Assessments:** These are required for high-risk AI or new data-processing activities. For instance, the EU AI Act requires a dedicated AI-impact assessment covering data quality checks, bias-mitigation strategies and transparency disclosures and should be updated whenever the model or its use case changes.

Failure to address these simultaneous demands can lead to "compliance creep," which refers to the ongoing influx of new rules and regulations that not only strain resources and teams but also increase the risk of non-compliance and vulnerabilities. This comes as the domino effect of new regulations for technologies like AI, continuously introduces fresh obligations and challenges.

The need for integrated compliance and risk management

In today's regulatory environment, where frameworks like GDPR, NIS2, DORA, and the AI Act increasingly

intersect, businesses can no longer afford to treat compliance and risk management as isolated functions. Siloed approaches, where legal, IT, security, and operational teams work independently, often lead to duplicated efforts, inconsistent risk reporting, and critical blind spots that undermine both efficiency and resilience.

To respond effectively, organisations must adopt a smarter, integrated model. Rather than maintaining fragmented policies and audit processes, forward-thinking enterprises are building unified compliance frameworks aligned with the most stringent regulatory requirements. For example, NIS2 mandates that organisations submit an early warning report within 24 hours of detecting a significant cyber incident. Meeting such standards requires a coordinated, cross-functional response. This shift calls for the adoption of modern Governance, Risk, and Compliance (GRC) platforms that provide centralised visibility into obligations, controls, and risks. A robust GRC strategy includes a unified risk taxonomy, enabling a common language for evaluating risks like data confidentiality or algorithmic bias, alongside cross-functional governance forums that bring together legal, privacy, engineering, and business leaders to review incidents and policies collaboratively.

Real-time compliance dashboards powered by automation and compliance-as-code tools allow organisations to monitor controls continuously, rather than relying on static quarterly reports. Additionally, integrated regulatory assessments streamline compliance by consolidating overlapping requirements, such as encryption, access management, and incident response, into a single, efficient process. Ultimately, integrated compliance and risk management not only reduce operational overhead but also enhance agility, transparency, and trust. By aligning governance models across teams and geographies, organisations can respond faster, report more accurately, and demonstrate a proactive commitment to regulatory excellence.

A strong foundational framework

One of the most effective ways to build a strong foundation is by leveraging established frameworks, chief among them, ISO/IEC 27001. This is the gold standard for information security management systems (ISMS), providing a globally recognised baseline for controls and continual improvement. Its flexibility allows organisations to scale security controls based on business context while maintaining a clear, auditable management system.

Whether it's extending to ISO 27701 for privacy, ISO 22301 for business continuity, or emerging standards for AI governance like ISO 42001, a strong ISMS enables organisations to manage overlapping requirements without duplicating effort. This integrated architecture simplifies audits, reduces control fragmentation, and ensures that governance remains consistent across departments and functions.

Its Annex A controls oversee access management, encryption, incident response and supplier security, which map directly to GDPR's data-protection mandates, DORA's ICT-risk expectations and NIS2's incident-management requirements.

Implementation steps

While implementing ISO/IEC 27001 is a valuable compliance exercise, it should also provide a strategic framework for building resilient, regulation-ready information security systems. The journey to achieve this begins with a clear scope definition: organisations must identify which systems, data types, and business units fall under regulatory scrutiny.

From there, a tailored risk assessment will guide the selection of Annex A controls, ensuring each control directly addresses specific regulatory clauses, such as implementing encryption at rest to meet GDPR Article 32 requirements. But certification is not the finish line.

Continual improvement is essential, driven by internal audits, management reviews, and key performance indicators (KPIs) like incident response times and vulnerability remediation rates. These metrics demonstrate compliance and foster a culture of accountability and agility.

Achieving ISO/IEC 27001 certification satisfies many converging regulatory demands by proxy and sends a powerful signal to customers and partners that the organisation is committed to global best practices in information security.

Looking ahead: the future of regulation & compliance

Looking ahead, the regulatory landscape will only become more interconnected, dynamic and fast moving. As AI technologies become more deeply embedded in everyday business functions, regulations are emerging that will demand new levels of transparency, explainability, and ethical oversight.

Governments and international organisations are pushing for AI systems that can be clearly understood, fairly used, and ethically governed. Requirements such as model documentation, bias detection, explainable logic, and algorithmic audit trails are no longer optional, they are becoming table stakes.

This calls for a transformation in how organisations assess and manage technology risk, embedding model governance and ethical review processes directly into the fabric of GRC programs.

By investing in integrated risk frameworks, aligning with global standards, and embedding governance into everyday operations, organisations can build lasting resilience. They can shift the narrative from regulatory burden to strategic advantage. In today's world digital trust is a key competitor differentiator.

Customers and partners are all paying closer attention to how organisations handle data, manage emerging technologies, and address ethical questions. Trust is won through transparency, compliance maturity, and a demonstrated commitment to responsible innovation. And businesses that embrace this mindset are getting ahead of the competition and laying the foundation for their future.

The convergence of global regulations shouldn't be seen as a challenge to overcome but as a catalyst for smarter, stronger, and more sustainable enterprise operations. Organisations that rise to meet this moment will redefine what leadership looks like in the age of intelligent systems.

How channel partners can address cyber threats, data centre constraints and cloud concerns

As cyber threats continue to evolve, data centre space constraints persist, and cloud adoption becomes more complex, financial institutions will increasingly rely on channel partners for their expertise.

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

FINANCIAL INSTITUTIONS have significant infrastructure challenges, in addition to all the economic uncertainty that continues at a global level.
The threat of cyberattacks against enterprise data infrastructure continues to escalate and the likelihood of an attack at some point is increasing daily. It's imperative that financial institutions build in more infrastructure level cyber resilience to minimise the impact of attacks by cyber criminals. At the same time, data centres are running out of space as financial enterprises reach full capacity but building new data centres may not be an option. The public cloud could be an option, but most find it's more expensive than they expected, plus there are additional risks with shared data centres.

These three challenges – cyber threats, data capacity, and cloud adoption, require a different approach and financial sector customers will be turning to trusted partners for guidance. Channel specialists should feel comfortable advising on a new combination of storage infrastructure strategies. They will be called upon to share practical insights and recommend advanced technological solutions that are best suited to financial industry clients. These will include banks, insurance firms, asset management companies, credit card providers, and other financial services companies, amongst others.

Here are some of the strategies and practical insights that channel partners providing enterprise storage for financial institutions need to be discussing with their clients.

Ransomware attacks against financial institutions are on the rise

Cyber resilience is critical for a financial institution's storage infrastructure, both to protect and defend its data against cyberattacks, but also to rapidly recover data in the event of a ransomware attack. According to Statista, from

MANAGED SERVICES SUMMIT NORDICS

21.10.2025

STOCKHOLM WATERFRONT CONGRESS CENTER

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

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

INDUSTRY INSIGHTS

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

NETWORKING OPPORTUNITIES

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

INTERACTIVE EXPERIENCES

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Angel BUSINESS COMMUNICATIONS

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

IT EUROPA

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

https://nordics.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS IT EUROPA ANGEL EVENTS

2021 to 2024, the share of financial institutions worldwide experiencing ransomware attacks increased significantly. In 2024, roughly 65 percent of financial organisations worldwide reported experiencing a ransomware attack, compared to 64 percent in 2023 and 34 percent in 2021.

To ensure the integrity of data being collected and processed – including bank account information, credit card information, client data and personal consumer information – banking and finance leaders need to navigate an ever more challenging security landscape.

Channel partners can play an important role in helping clients to understand the key to fighting off a cyberattack - having a known clean copy of data that can be recovered before the cyberattack has any significant impact. Getting this in place requires an enterprise storage strategy that is supported by cyber detection, automated cyber protection, encryption, access management controls, capacity consumption thresholds, guaranteed recovery time objectives (RTO), and data testing. At the same time, this strategy needs to comply with regulatory requirements.

Channel partners with clients in the financial services sector will appreciate that financial institutions have some of the most stringent cyber resilience and security requirements. These clients will need the assurance of compliance-optimised and resilient cyber recovery storage solutions, proven for use inside banks and other large financial institutions. To properly protect the enterprise's primary storage, these cyber resilient storage solutions will need a range of vital elements including:

- **Immutable snapshots –** these can be automatically generated, time scheduled or manually created but must all share the common features of being secure and unchangeable, point-in-time copies of primary data.
- **Logical remote and local air-gapping –** to provide a simple way to separate immutable data copies from network access, either locally, remotely, or both.
- **Fenced forensic environment –** enabling the creation of a completely private network that is isolated for data validation, testing, and recovery.
- **Cyber detection –** to validate the integrity of immutable snapshots using powerful, AI-based scanning engines.
- **Automated cyber protection –** this reduces the threat window for cyberattacks, enabling seamless integration into an enterprise's SOC, SIEM, or SOAR cyber security applications.
- **Near-instantaneous cyber recovery –** ensuring that all known good and validated data can be recovered and available for restore in minutes, regardless of the data set size.

When channel partners combine all these elements into an enterprise storage strategy, they all come together to build and enhance the cyber resilience of a financial institution's data infrastructure. Having a broad set of cyber capabilities for both primary and secondary storage will ensure financial institutions can combat ransomware and malware attacks far more effectively.

Balancing data centre capacity constraints with public cloud concerns

Many financial institutions are understandably reluctant to build new data centres due to high construction costs and constant technological shifts. It is financially more viable to maximise the space available within existing data centres. At the same time, many have an interest in leveraging public cloud services, but face very legitimate concerns about the long-term costs and potential loss of data control and security.

Channel partners can play a crucial advisory role here, supporting their financial industry clients with critical decision making over which direction they should take. In many instances, this will involve a combination of the two. Firstly, identifying how to provide the largest possible storage capacity in a fraction of the size of traditional storage arrays and thus making the best possible use of available data centre space. Secondly, by enabling clients to benefit from an end-to-end, hybrid multi-cloud experience in which the use of public and private clouds together is completely seamless.

Channel's role in future-proofing financial infrastructure

As cyber threats continue to evolve, data centre space constraints persist, and cloud adoption becomes more complex, financial institutions will increasingly rely on channel partners for their expertise. By providing a comprehensive strategy that incorporates cyber resilience, storage optimisation and a balanced, cost efficient and secure cloud approach, solution partners can help their financial clients to build a future-proofed enterprise storage infrastructure. And ultimately, the channel partners that offer forward-thinking, compliance-driven enterprise storage solutions will not only generate immediate value for their clients, but also establish themselves as indispensable technology partners for financial data security and management.

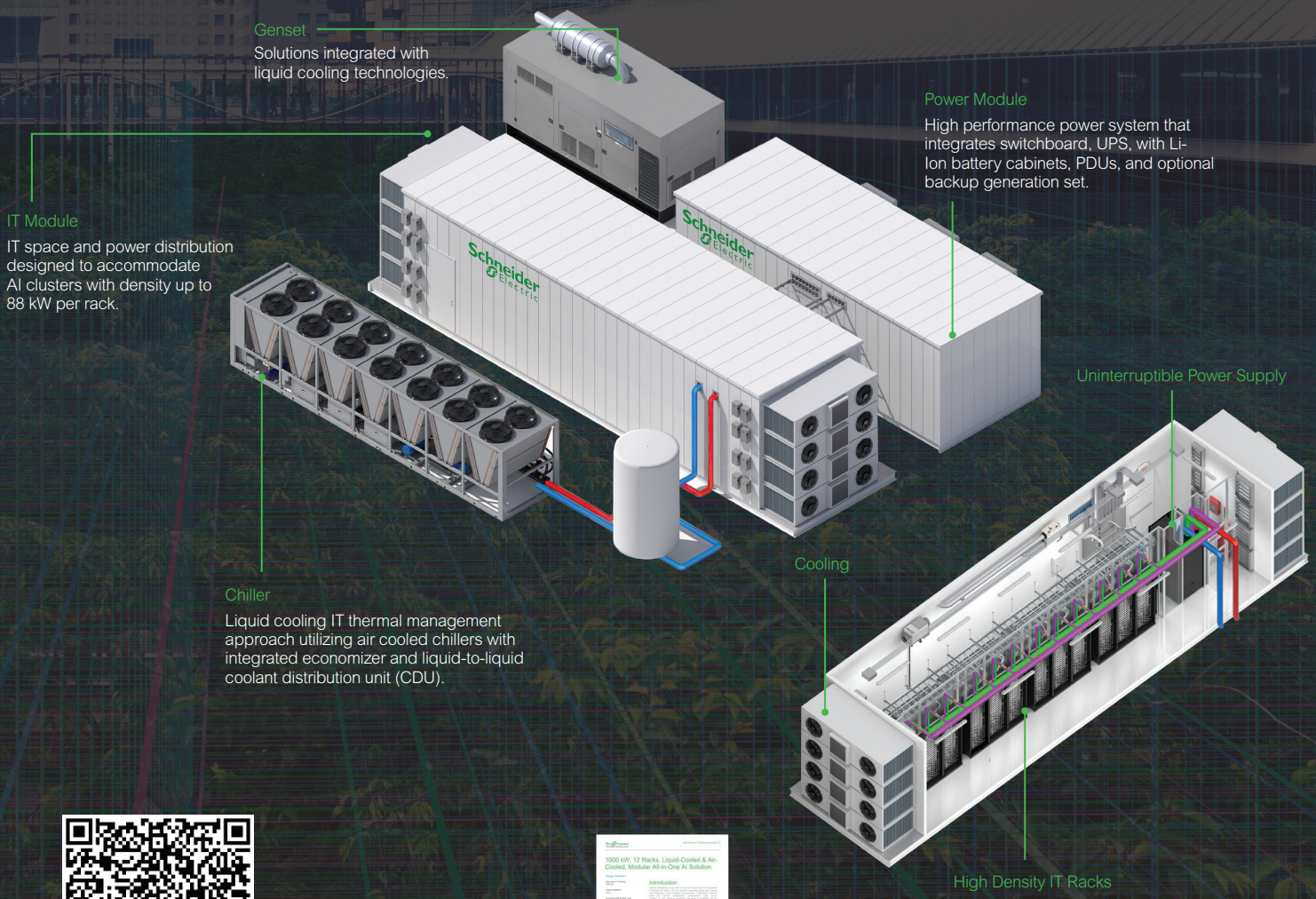
Why wait to build an AI data center when you can unpack one now!

Are you ready to revolutionize your AI infrastructure with modular data centers?

Modular AI data center from Schneider Electric present a prefabricated, scalable infrastructure solution tailored to meet the extreme power, cooling, and density demands of generative AI workloads. Discover how prefabricated modular data centers can accelerate AI adoption, simplify design and construction, and support sustainability strategies.

Download the e-guide and reference designs

to learn more how Schneider Electric's Modular AI Data Centers address these critical challenges and help you stay ahead in the evolving technological landscape!



Download the e-guide

Life Is On Schneider Electric

How can channel businesses reduce customer downtime

When a routine update rendered over eight million global software applications unusable, the American cybersecurity company concerned was thrown into the spotlight. The worldwide incident not only deprived businesses of access to critical tools but also underscored a pressing concern: what can companies do to mitigate downtime when systems are inherently fallible and outages are often beyond their control?

BY MICHELLE WOULD, DIRECTOR OF CUSTOMER EXPERIENCE AT AGILITAS

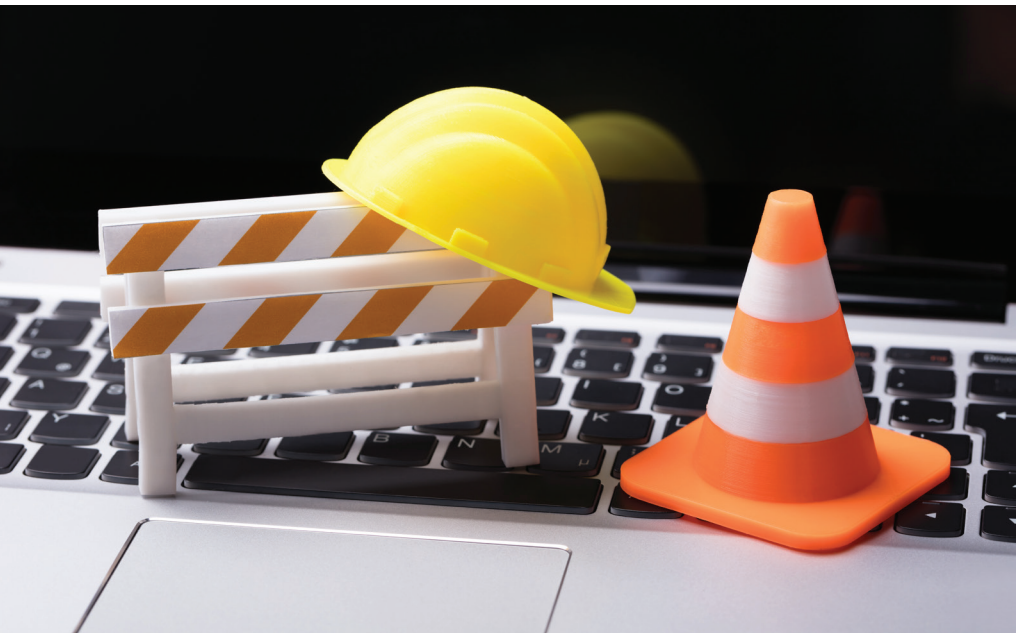
THE INCIDENT, which had an estimated economic cost between $300 million and $1 billion, mirrored similar large-scale hardware outages such as the Salesforce DNS disruptions earlier this year, which left countless businesses unable to access critical tools and customer data, severely impacting their daily operations and client interactions.

The unpredictability of these disruptions has highlighted why organisations need to ensure their customer support strategies can withstand potential causes of downtime.

Why customer downtime is an economic threat

According to recent statistics, 20% of businesses in the UK experienced more than three internet outages in the last year with an expected £17.6 billion economic loss due to connectivity issues.

Cybersecurity glitches, hardware failures, poor internet connectivity and software failures are just some of the causes of operation shutdown which can disrupt workflows, increase costs and affect clients.



Beyond immediate financial losses, prolonged outages can erode customer trust, leading to clients seeking more reliable alternatives to reduce the impact on long-term growth. Channel businesses which rely on a smooth service flow face additional risks, especially as partners and end-customers expect seamless, uninterrupted operations. However, outages can strike at any time. As a result, businesses must be equipped with a clear plan of action that addresses both short-term risks and builds long-term resilience.

The role of customer experience in reducing downtime

To manage customer downtime effectively, channel businesses must prioritise transparent communication, agility, and resilience—all of which are integral to delivering a positive customer experience. When downtime occurs, clear and timely communication ensures customers stay informed, minimising frustration and enhancing trust. Agility plays a key role as well, allowing businesses to quickly switch to alternative resources when systems fail, reducing the impact of disruptions. Resilience, built through robust infrastructure, dependable partners and proactive strategies, helps businesses recover swiftly while minimising vulnerabilities.

Adopting a proactive approach to downtime prevention is crucial. By integrating processes designed to identify and mitigate potential risks, channel partners can stay ahead of issues before they escalate. Investing in team training is equally important; upskilling staff ensures they understand the right protocols for managing different types of outages, equipping them to respond effectively and safeguard operations. This combination of preparation, agility, and skill not only helps minimise downtime but also strengthens customer relationships, reinforcing trust and ultimately safeguarding the business's reputation.

Proactive strategies to reduce hardware downtime

While downtime's unpredictability makes it difficult to prepare for, businesses can take proactive measures to minimise its effects. Hardware failures, often a key cause of outages, require robust contingency plans, including regular maintenance schedules and rapid-response protocols. Collaborating with channel partners who can provide reliable hardware solutions and responsive support ensures that organisations have suppliers they can rely on during critical periods, offering replacements or repairs and minimising the risk of extended disruptions.

Leveraging automatic failover systems is another key strategy, as these systems can shift workloads to backup hardware during failures and can help maintain continuity across hardware platforms. Channel organisations can also leverage cloud-based infrastructure to strengthen resilience, allowing them to distribute servers and enable operations to continue even if a single server experiences issues.

According to Statista, staff incompetence and failure to follow correct procedures ranked among the top two reasons for global IT outages.

Automating response times can also help reduce the likelihood of human oversight during outages by triggering essential systems, keeping clients informed and alerting technical teams immediately. Without automation, businesses risk facing longer periods of downtime and a less coordinated response.

Moving forward

With service reliability increasingly linked to customer trust and loyalty, channel organisations must be prepared to handle hardware disruptions that threaten operational continuity. Hardware failures due to outdated infrastructure, manufacturing defects or unexpected breakdowns can cause significant disruptions to processes. By leveraging a holistic multi-layered strategy which incorporates proactive hardware maintenance, collaborative partnerships, data security, automation, cloud-based infrastructure, and regular backup systems, companies can effectively mitigate the effects of unexpected outages.

Technology alone can't mitigate supply chain risk, but strategic partnerships can

The disruptions of 2025 have laid bare critical vulnerabilities across global supply chains. Nearly 19% of breaches now stem from supply chain attacks, with average costs exceeding $4.7 million. As we all know, these incidents don't just disrupt operations. They undermine the foundational trust that businesses are built on.

BY LORENZO ROMANO, CEO OF GCX MANAGED SERVICES

THE good news is that businesses are not facing these challenges alone. Over the past few years, Managed Service Providers (MSPs) have evolved from tech support to fully end-to-end strategic partners. They now work closely with leadership, helping organisations adapt to regulatory changes and operational risks and strengthen long-term resilience.

Visibility fuels regulatory adherence

Achieving visibility across supply chains remains a consistent challenge for many organisations. Data is often dispersed across various systems, making it difficult to detect issues before they evolve into significant operational disruptions. While cloud computing has become indispensable to today's supply chain infrastructure, gaps in transparency, access management and security controls still leave many businesses exposed to huge risk.

Cloud-native solutions such as Secure Access Service Edge (SASE) are increasingly vital in addressing these challenges. By integrating networking and security functions into a unified platform, SASE helps organisations streamline oversight and improve access controls throughout cloud and IoT environments. This not only strengthens security but also breaks down data silos, which is an essential step for maintaining compliance with evolving regulatory requirements.

MSPs are essential partners in rolling out and maintaining the likes of SASE solutions. Their technical know-how enables them to navigate the complexities of setup, integration and long-term management, allowing companies to strengthen their supply chain security without expanding internal IT teams. Just as importantly, MSPs offer localised regulatory insight, ensuring businesses are aligned with compliance requirements across regions.

The importance of adopting Zero Trust

SASE's advanced visibility capabilities also lay the groundwork for adopting Zero Trust security principles. By delivering insights into network behaviour, organisations can implement continuous validation of users and devices, ensuring that only verified entities gain access.

This approach is particularly vital in the context of global supply chains, where operations stretch across borders and involve third-party partners. The sheer scale and complexity of these ecosystems introduce countless endpoints that must be monitored.

Zero Trust mitigates this risk by enforcing strict, ongoing authentication for every user, device and application, regardless of their location. Reflecting this growing need, Gartner forecasts that by the end of 2025, 60% of enterprises worldwide will have embraced Zero Trust architectures, a sharp rise from 20% in 2022.

MSPs are key enablers of this transition. Their global reach and strong vendor networks position them to guide organisations through the deployment and management of Zero Trust frameworks, bolstering defences against increasingly sophisticated cyber threats.

The role of MSPs in building resilient supply chains

Sustained growth isn't achieved through technology alone. It also relies on the strength and flexibility of the entire network of partners and suppliers that support a business.

MSPs play a crucial role here, empowering organisations to rethink and redesign their supply chain operations for greater resilience.

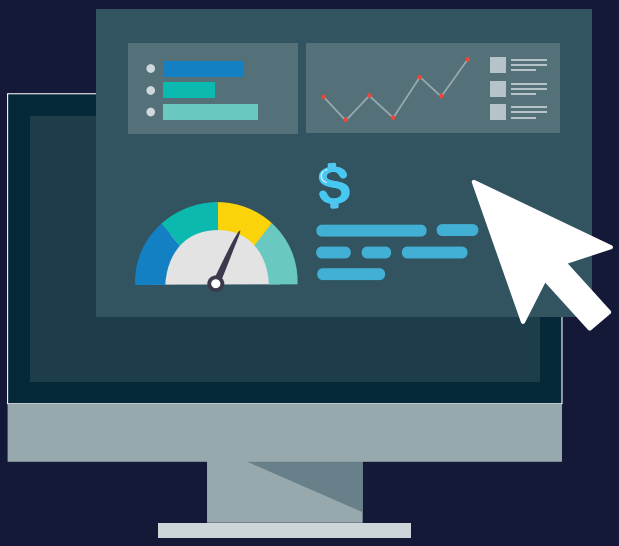
Gone are the days of simply offering IT assistance; MSPs now well and truly help organisations diversify their supplier base, implement adaptable technology solutions and nurture the kind of collaboration essential for staying ahead in unpredictable markets.

By partnering with agile and innovative suppliers, companies of all sizes can better navigate disruptions and keep their operations moving, no matter what the market throws their way.

datto
A Kaseya COMPANY

Boost MSP Productivity & Profitablity with Datto BCDR

Reduce downtime, streamline operations & grow recurring revenue.



LEARN MORE

www.datto.com/partner-request/bcdr

Investing in the right tech now will safeguard your business to meet future AI needs

The AI revolution has taken the world by storm, shaking up a whole range of industries – from healthcare and finance to VR gaming and predictive social media analytics, the impact is huge. But with machine-learning tools now commonplace, the data demand facing organisations has skyrocketed. And some businesses are struggling to keep up with the pace. With no signs of the progress slowing down, the ability for organisations to adapt their data processing capacity is vital.

BY ALASDAIR STAPLETON, PRODUCT MANAGER AT ETB TECHNOLOGIES LTD

While the temptation is always to deal with what's immediately in front of you, planning for growth in capacity can save time, effort and money in the long term. What's more, from a strategic point of view, embedding scalability can prove an extremely effective way to gain a head start over competitors, rather than constantly just aiming to keep your head above the rising tide of data.

Supporting evolving data processing needs

Often, businesses are so focused on the "now" they forget to consider how their computational and storage needs may evolve in future. As workloads increase, companies must ensure their infrastructure is scalable and versatile enough to adapt, without requiring a complete system overhaul.

A system that can grow with the needs of your business, while supporting current workloads, is key. What's required for this growth will differ between organisations – some might need larger memory or storage capacity, while others will rely on greater processing power.

For example, as AI and high-performance workloads grow, so do processing demands. If a business invests in a server chassis design that supports only one or two GPUs, it may struggle to up its processing power without a complete replacement. This shortsighted approach can lead to wasted time and money - costs that can be easily avoided by opting for a server with a higher core count from the start.

Whatever the exact specifications might be, the point is that being able to make modular upgrades is vital to efficient scalability, so investing in hardware that allows this from the outset makes sense. But it's important to note increased performance demands also bring additional considerations, such as increased power and cooling requirements. It's crucial to account for these factors early in the planning stage to avoid unanticipated future limitations.

Ensuring compatibility to avoid manufacturer lock-in

Buying equipment without considering its ability to integrate with other products can be a glaring oversight. High performing systems have multiple moving parts. When built correctly, the benefits can be lifechanging. But being too quick to hit the "buy now" button, without properly examining the

compatibility of these different parts, can lead to major logistical challenges. While certain components – like GPUs, memory and network cards - tend to be interchangeable across manufacturers, some brands and products are more limited.

Just like Apple, which has drawn us into its exclusive product ecosystem, server-specific products like motherboards are often incompatible with other brands, leaving little choice when it comes to system upgrades. This means companies don't have the freedom to mix and match different parts, customising their IT infrastructure to their exact needs. For businesses with unique and diverse specifications, universally compatible IT components could be a safer option to support future advancements.

Optimising for AI now to mitigate long-term costs

As AI and machine learning becomes more integrated into our everyday working lives, the technology we use must be geared up for these workloads. However, optimising your server set up to cope with future tech upgrades, growth and strategic level changes requires financial commitment. The good news is that investing in the right technology to support future growth now means you won't need to start from scratch and bear the brunt of even bigger costs later. As budgets continue to be squeezed, there are also steps you can take to reduce the overall expense.

In addition to ensuring you spend smartly to avoid spending twice, assessing what options you have for sourcing equipment can also result in a significant saving. For example, organisations often overlook refurbished technology as a viable option for future-proofing. This can be short sighted as refurbished hardware provides enterprise-level performance at a fraction of the cost.

Assuming you're using a reputable and trusted supplier, refurbished systems undergo rigorous testing and come with warranties, ensuring they perform as expected. This means there should be no concerns when it comes to reliability or performance levels. What's more, buying refurbished extends hardware lifespans, reduces electronic waste and supports sustainability goals. With green credentials becoming more and more important to businesses this can be a valuable proof point.

The big picture

Future-proofing IT infrastructure is essential for businesses competing in an increasingly technology-driven world. By prioritising scalability, compatibility, and AI optimisation, while considering refurbished technology, organisations can make strategic investments that offer long-term value.

Assessing what a business needs now, as well as what it might need in the future, is crucial to making sustainable, cost-effective decisions. It may not be possible to know exactly what's coming round the corner, but taking steps to future-proof your technology stack means it is possible to be ready for it.

Why MSPs shouldn't fear data-centric security

Today, managed service providers (MSPs) have a tremendous opportunity to capitalise on growing demand for cybersecurity and data-centric security services. In fact, according to Canalys, 90% of cybersecurity solutions will be delivered by channel organisations in 2025—that translates to over £200 billion in revenue.

BY PETER BRADLEY, PRODUCT STRATEGY LEAD, AVEPOINT

IN SPITE of the size of this opportunity, many MSPs are reluctant to expand their involvement in the data-centric security market. In most cases, this fear comes from the perceived complexity of delivering data security-related services. But it's important for MSPs to understand that, unlike in-house security teams at smaller organisations, they have access to the critical expertise, staff, and technology needed to deal with the challenges of securing data in the age of AI, which has created new security risks (87% of organisations faced an AI-driven cyberattack last year, according to one study). That's why the complexity of data-centric security is really an opportunity for MSPs, and here's how they can work to expand their businesses effectively in years to come.

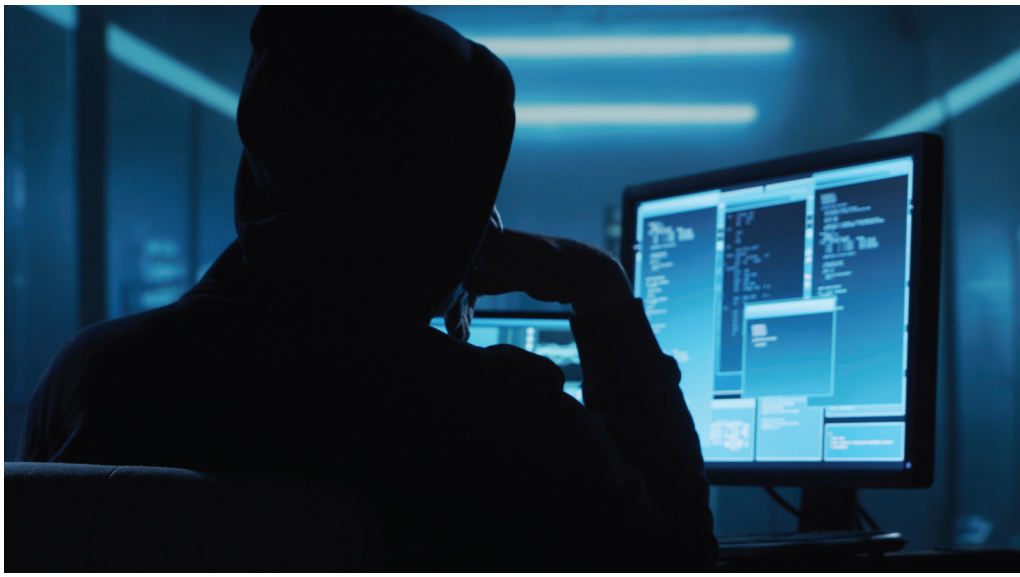
Why data-centric security complexity means opportunity for MSPs

Before the arrival of the cloud, cybersecurity professionals and teams were broadly focused on perimeter security (securing the periphery of their environments from external threats) which meant adding protections to assets like user accounts, infrastructure, and on-premises servers. This was a logical and sound approach 10, 15, or 20 years ago, when the threat landscape was radically different from what it is now. While this approach is still important, the rise of AI and cloud collaboration, the evolution of insider threats, and the arrival of an increasingly sophisticated threat landscape has shifted the focus of cybersecurity inward to the data itself.

Why? Data-centric security poses a fundamentally new set of challenges. Instead of simply trying to protect infrastructure from malicious external actors, data-centric security is much more focused on controlling who has access to data, regulating the flow of data within a particular organisation, protecting data from both accidental and malicious insider threats, and other related issues, which also include highly advanced external threats including AI-driven malware or ransomware, social

engineering attacks, and more. Many organisations rightly view this work as complicated and may lack the skills, technology, and expertise to navigate it effectively in-house. However, most MSPs don't face these same challenges. Unlike their customers, MSPs have specialised staff, expertise, and (importantly) technology to navigate the complexities of today's data-centric security challenges.

This is why MSPs shouldn't fear complexities of data-centric security in the same way as their customers: they have the tools needed to tackle these challenges in a safe, effective, and profitable way.



How MSPs can solve today's data-centric security problems

Given the shortage of in-house skills, expertise, and technology needed to deal with today's increasingly sophisticated data-centric security threats, MSPs must now play a critical role in addressing today's data-centric security challenges.

To effectively safeguard their clients, MSPs should adopt a proactive and layered approach, including continuing to execute the fundamentals of perimeter, system, device and user account protection. Simulated phishing exercises and , security awareness training are vital in minimising human error, which accounted for a staggering 95% of security breaches in 2024, according to a report from Mimecast. But they must now go further to include measures which protect the data itself.

Data Security Posture Management (DSPM) tools and data governance techniques such as detection and remediation of overshared data, ROT (redundant, obsolete or trash) data, unclassified data, regular access reviews and workspace renewals are all becoming essential for ensuring that security defenses remain robust against new and emerging threats related to the arrival of AI technology.

MSPs should also prioritise educating their clients on best practices for data-centric security. Initiatives like appointing data owners within the business, supporting them to take responsibility for the data they are closest to, and framing the ongoing governance of data as a responsibility that must be shared between the business and IT.

Put simply, "security is everyone's responsibility" needs to be more than just a cliché! Shared accountability is crucial for data-centric security to be effective. By equipping their clients with knowledge and enforcing secure behaviors, MSPs can help create a culture of vigilance.

Automated tools for managing compliance and data-centric security posture are also key for meeting regulatory standards like GDPR and the EU AI Act. MSPs can leverage DSPM tools to help their clients stay audit-ready. This not only reduces risks but also strengthens client trust.

By combining expertise, automation, and education, MSPs can rise to meet the growing challenges of clients' data-centric security while reinforcing their value as indispensable partners in safeguarding sensitive information.

It's up to MSPs to secure the future of data

In an era of increasingly complex data-centric security demands, MSPs are uniquely positioned to turn challenges into opportunities. By combining advanced technologies, specialized expertise, and proactive client education, they can not only address today's sophisticated threats but also build lasting trust and business growth.

The path forward lies in embracing the intricacies of data-centric security as a realm where MSPs can differentiate themselves and thrive as indispensable allies to their clients.

Before the arrival of the cloud, cybersecurity professionals and teams were broadly focused on perimeter security (securing the periphery of their environments from external threats) which meant adding protections to assets like user accounts, infrastructure, and on-premises servers. This was a logical and sound approach 10, 15, or 20 years ago, when the threat landscape was radically different from what it is now

Beyond encryption: the new face of ransomware threats

A major shift is happening in the world of cybercrime, reshaping how organisations must think about digital threats.

BY LORRI JANSSEN-ANESSI, DIRECTOR OF EXTERNAL CYBER ASSESSMENTS AT BLUEVOYANT

CYBERCRIMINALS continue to exploit organisations for financial gain using phishing, social engineering, malware attacks, and data theft to deploy ransomware.

The UK's National Crime Agency predicts that 2025 could be the worse year on record for ransomware attacks in the country, with the vector now viewed as a critical national security threat.

This presents a triple threat for organisations: exposure of confidential data, reputational damage, and escalating regulatory fines. However, ransomware has now evolved to the point that attackers no longer need to encrypt files to inflict crippling damage.

As a result, organisations need to ensure that their internal IT and cyber security teams are aware of the consequences of encryption-less extortion.

Extortion without encryption

Instead of locking files, this allows attackers to prioritise data theft and the threat of public exposure. They are now focusing solely on exfiltrating sensitive information and using it as leverage to leak or sell data. This method is faster, stealthier, and exponentially more destructive, challenging not just IT departments but boardrooms and communications teams alike.

And it's becoming increasingly popular. According to a recent Honeywell report, there was a 46% increase in ransomware extortion between October 2024 and March 2025.

A key element of double and triple extortion schemes involves attackers not only demanding a ransom for stolen data but also applying additional pressure through Distributed Denial-of-Service (DDoS) attacks, or by contacting the victim's customers and partners.

Instead of solely encrypting data and threatening leaks, attackers now aim to compromise broader networks, making the tactic faster and harder to detect, since data exfiltration is less likely to trigger security alerts than large-scale encryption.

However, despite the pressure to pay the ransom, doing so may only encourage threat actors to attempt future attacks, and the return of stolen data is never guaranteed.

The new cyber arms race

Threat actors are now weaponising AI to generate highly convincing phishing emails, map digital infrastructures, and pinpoint vulnerabilities with unprecedented speed and accuracy. AI allows ransomware to move faster and hit harder, stretching already pressured security teams to their limits. As these technologies become more accessible, the window to defend against them is narrowing.

What every organisation must do

To mitigate the risks associated with ransomware and other cyber threats, organisations must adopt a multilayered approach to resilience. A foundation of this strategy is the regular backing up of critical data and systems. These backups should be securely stored offline and encrypted to avoid risk of compromise.

By undertaking routine testing of both backup and restoration procedures, organisations can ensure they function reliably in real-world incident scenarios. By embedding these practices into an overarching cyber resilience framework, organisations can dramatically improve their ability to recover swiftly and securely from attacks.

Furthermore, organisations should create, maintain, and frequently exercise a cyber incident response plan that includes clearly defined procedures for responding to ransomware attacks. Regular testing of this plan helps to identify and address any potential gaps.

Identity and Access Management

The deployment of strong Identity and Access Management (IAM) solutions is fundamental to defending against ransomware attacks. This includes implementing multi-factor authentication (MFA) across all services, particularly for remote access points such as VPNs and webmail, as part of a multi-layered approach.

User and administrator privileges should be tightly controlled, granting access only to the resources necessary for each role. Adopting a Zero Trust architecture further reinforces this strategy by mandating continuous verification of every user and device, regardless of their location or level of access. This ensures that trust is never assumed, and security remains uncompromised.

Simultaneously, centralising all operating systems, software, and firmware up to date is essential to patch known vulnerabilities that cybercriminals often exploit. Network segmentation should also be prioritised to isolate critical systems. By dividing the network into secure zones, organisations can limit the lateral movement of ransomware, reducing the risk of it spreading from an infected device to high-value infrastructure.

Employees on the frontline

The human factor is crucial in any cyber security strategy. Employees serve as both the frontline defenders and the final safeguard against threats. Organisations should therefore be prioritising training that helps employees to identify phishing attempts, social engineering tactics and unusual activities within the system. It has become a strategic necessity, far beyond simply ticking a compliance box, rather than an investment in organisational resilience and brand reputation.

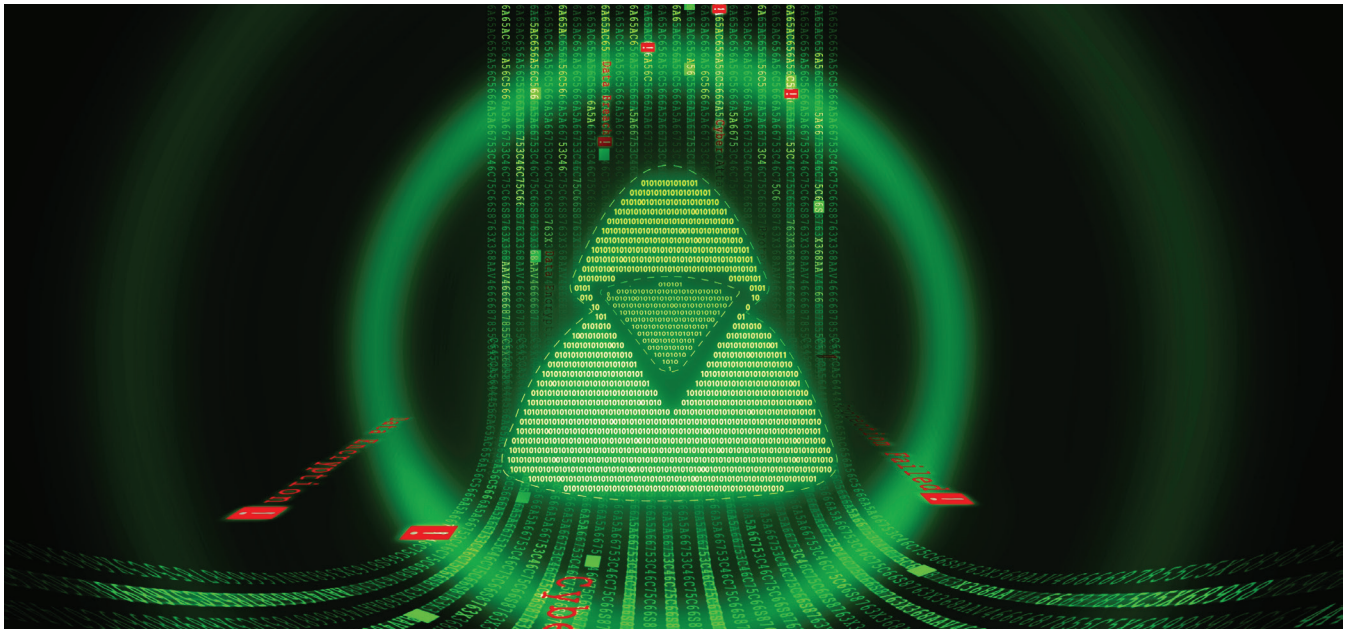
Building proactive ransomware defences

To stay ahead of ransomware threats, organisations need faster detection and response tools. Deploying Endpoint Detection and Response (EDR) tools is essential; these advanced systems catch suspicious behaviour that traditional antivirus often misses. By using real-time behavioural analysis, EDR helps teams spot and act on unusual activity before it spreads. Once a threat is identified, speed is everything, therefore, organisations should isolate infected devices immediately and bring in internal or external incident response experts to contain and recover. Also, they should report the attack to the authorities, providing valuable intelligence that will help to disrupt the broader ransomware ecosystem.

As cyber threats grow in sophistication and scale, resilience must evolve beyond traditional system recovery. True cyber resilience encompasses more than technical defences; it demands proactive reputation management, clear and transparent communication, and well-coordinated response strategies.

By embedding resilience into the core of their cybersecurity frameworks, organisations can not only reduce the impact of cyber incidents but also preserve stakeholder trust and ensure business continuity.

With foresight and preparation, leaders can outpace adversaries, positioning their organisations to respond swiftly, confidently, and effectively when it matters most.



Powering the future of AI, cloud & real-time applications with wavelength

In today's instant and online world, demands for cloud, AI, and real-time applications are higher than ever, with a growing number of uses cases across multiple enterprise verticals. As these digital services and experiences grow, enterprise customers and end users will not tolerate poor online experiences, making network performance a key requirement when building and enhancing their business infrastructure.

BY MARK DALEY, DIRECTOR OF DIGITAL STRATEGY & BUSINESS DEVELOPMENT, EPSILON TELECOMMUNICATIONS

IN ORDER to support this growth, the global service provider network infrastructure market is expected to reach a staggering $174.1 billion by 2028 according to KBV Research. There is a huge market opportunity for service providers to better serve enterprise demands with networking that can provide competitive advantages thanks to high performance.

Strong and stable connectivity is especially crucial for mission-critical use cases that demand high-capacity, low-latency connectivity, including real-time financial trading, large-scale data transfer, cloud access, network expansion, application orchestration and content delivery.

Legacy networks can no longer keep up with the growth and performance demands of today's business landscape, making high-capacity, low-latency alternatives critical. Wavelength is increasingly being adopted by service providers to build private, high-speed data pathways between critical locations, data centres, and cloud environments across the globe. It is specifically designed to transport data over long distances, allowing for high-capacity, scalable, and efficient data transmission.

It is a huge market with growing opportunities, expected to reach over $8.1 billion by 2028 according to The Business Research Company. As more businesses seek to modernise their connectivity to stay agile and

competitive, it is critical for service providers to futureproof their network infrastructure, reduce latency, and support emerging use cases to meet the demands of tomorrow.

Coping with connectivity demands

With data volumes skyrocketing and customer network requirements becoming more complex, keeping up with demand can be a struggle – especially for network operators with a legacy network.

This has created a dual market challenge. On one side, network operators need to upgrade their core infrastructure to handle rising traffic and technical demands. However, upgrades to legacy infrastructure can be costly and complex, with traditional networks often being rigid and difficult to scale. On top of this, many traditional networks are not designed for integrating application between clouds – a crucial need for many enterprises.

Ethernet and similar network types can easily become congested if traffic levels on the common network hit peak capacities, leading to performance issues and dissatisfied customers. To stay ahead, service providers must scale their networks while also making them smarter, to support the heavy lifting of core infrastructure.

On the other hand, network operators face surging bandwidth needs from customers that are frequently streaming and using cloud and other internet services located outside of the network operator's own network. Today's enterprise customers and end users expect fast, reliable access to everything, from real-time applications and cloud services to high-definition streaming, wherever the content or application is located.

To extend their network and support the growing demands of end-user services, service providers need a strategic approach via partnerships and interconnected network operators who can match their speed and bandwidth needs.

Getting on the right wavelength

The connectivity technology addressing all of the growth needs of a network operator is Wavelength – a technology that efficiently transmits data through fibre optics. Optical networks often use Dense Wavelength Division Multiplexing (DWDM) technology to send multiple signals simultaneously along the same fibre, via different wavelengths of light.

DWDM is crucial for meeting the growing demand for high-speed internet, video streaming, high-bandwidth applications, data centre interconnection (DCI) and cloud services, while enabling flexible bandwidth expansion without extensive infrastructure changes. It can also support Ethernet interfaces at end points, making it a perfect option for enterprise networks.

It offers transparent, point-to-point, private, dedicated and secure connections that can be tailored to meet specific business needs, ensuring fast, reliable communication to future-proof network growth.

Some other benefits include:

- **Rapid Connectivity –** Fast and efficient connections, with quick data transmission across long distances to swiftly respond to market demands.
- **Scalable Bandwidth –** Simple to scale bandwidth according to growing customer requirements, without causing headaches in terms of infrastructure constra
- **Guaranteed Quality –** Guaranteed throughput, low latency and low jitter connections, providing a reliable, high-quality experience, every time.
- **Flexible Options –** Different options of service resilience, including Unprotected, Diverse and Protected. Service providers can choose the solution that best fits their needs in terms of cost and security.
- **Cost Efficiency –** Significant cost savings in comparison to other options such as Dark Fibre, thanks to optimising network bandwidth.

Partnering for long-term success

An expert partner can hugely simplify service provider network upgrades, with all the tools, expertise and insights needed for long-term success with wavelength.

Some important factors to consider include:

- **Global Reach –** The right networking partner will have a carrier-grade, hyper-scalable global backbone that interconnects the world's leading communications and technology hubs, including data centres, cloud providers and interconnection points.
- **Network Expertise –** As the industry evolves, having a partner with decades of experience is invaluable. They need to understand the current landscape, but also anticipate future trends and challenges.
- **Simple Management –** An intuitive online portal can simplify the setup and management of networking services from a single location.
- **Competitive Pricing –** It is important to look out for competitive pricing, without compromising on service quality.
- **Robust Infrastructure –** A reliable networking partner will provide a robust network backbone that prioritises redundancy and reliability, designed to prevent failures and ensure uninterrupted service.
- **Security –** The right partner will implement the latest security measures and continuously monitor the network for potential vulnerabilities and threats, with a dedicated team of cybersecurity experts.

Future-proofing networks

The demand for high-bandwidth applications and faster, more reliable networks, has never been higher. For today's service providers, connectivity is increasingly defining success.

With legacy infrastructure unable to keep up with the requirements of more digitally savvy businesses and end users, different connectivity options are vital to increase reliability and redundancy across global networks.

Wavelength is a powerful solution to expand network capacity and performance, while opening new opportunities for growth and improved service delivery.

By working with an expert network partner, service providers can optimise their networks, scale with confidence, and stay ahead of the competition to unlock new levels of growth in a rapidly changing market.

Why business continuity is the growth engine MSPs can't ignore

datto
A Kaseya COMPANY

Learn how MSPs are driving growth and boosting MRR by prioritizing business continuity with Datto's purpose-built BCDR solutions.

THE conversation is no longer about backups; it's about business continuity. Downtime has become an existential threat for organizations, especially small and midsized businesses (SMBs). Cyberthreats like ransomware are evolving faster than most SMBs can keep up with, and extreme weather events and system outages are hitting more frequently. For an SMB generating $10 million in annual revenue, even a single day of downtime can result in losses of up to $55,000. That's why more and more SMBs are shifting their focus from backup to business continuity.

According to the State of BCDR Report 2025, over 50% of organizations are planning to switch their primary backup provider, citing limited disaster recovery capabilities as a major concern.

As businesses prioritize continuity, managed service providers (MSPs) must respond with a strategic pivot of their own.

MSPs that move beyond selling backups and start delivering true business continuity will not only boost client satisfaction and retention but also tap into stronger streams of monthly recurring revenue (MRR).

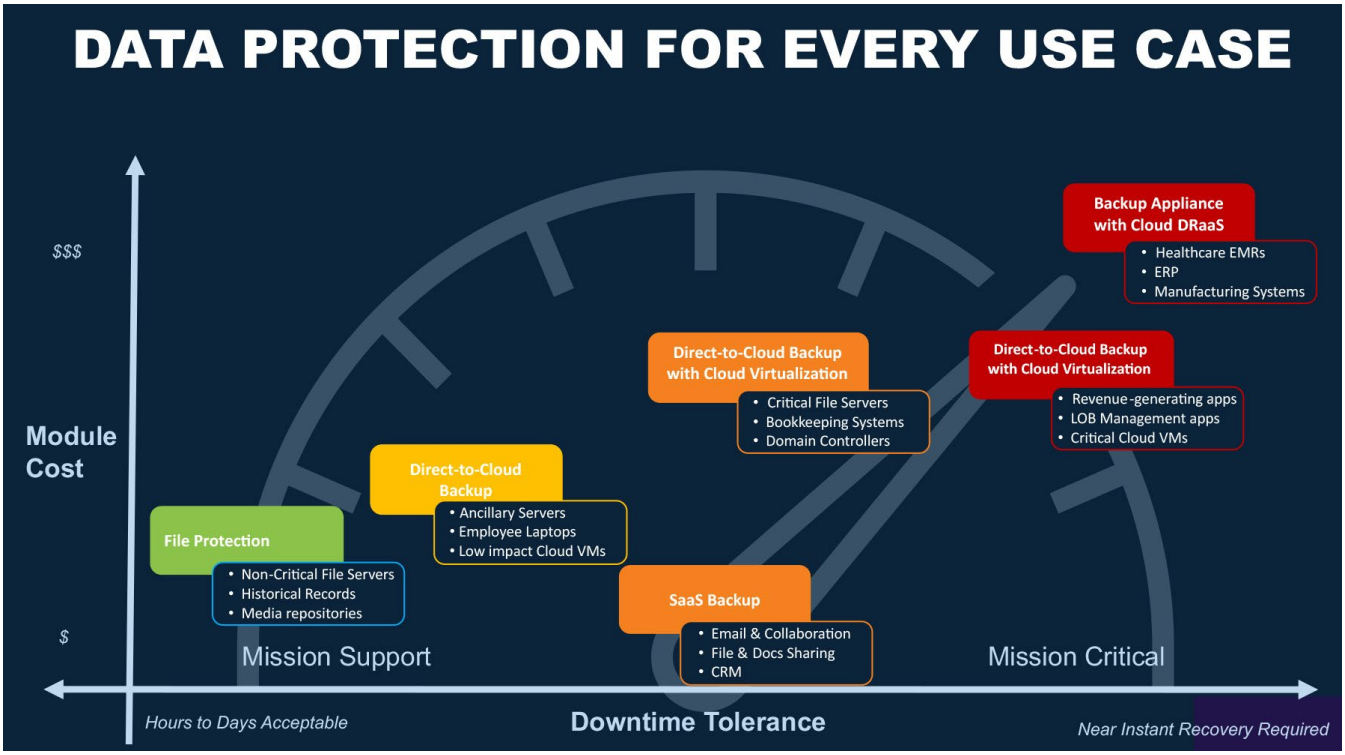
Businesses are willing to pay a premium for solutions that keep them operational and resilient. That's why it's time for MSPs to start treating business continuity and disaster recovery (BCDR) as a growth engine. In this article, we'll explore how MSPs can take advantage of this growing demand and turn BCDR into a powerful driver of long-term profitability.

How MSPs are boosting profit margins with BCDR

MSPs worldwide are increasingly weaving BCDR into their core service offerings. According to the State of the MSP Industry 2025 Look Ahead report, the most profitable MSPs — those generating over $10 million in revenue — are already bundling BCDR with managed security services.

Unlike break-fix work or one-off projects, BCDR is delivering stable, recurring revenue streams that help MSPs scale with predictability. It's also emerging as a top standalone service, with 46% of MSPs offering BCDR as a key part of their portfolio.

Let's explore different strategies MSPs adopt to leverage BCDR and boost their margins:



➤ Figure 1: Provide data protection for every use case

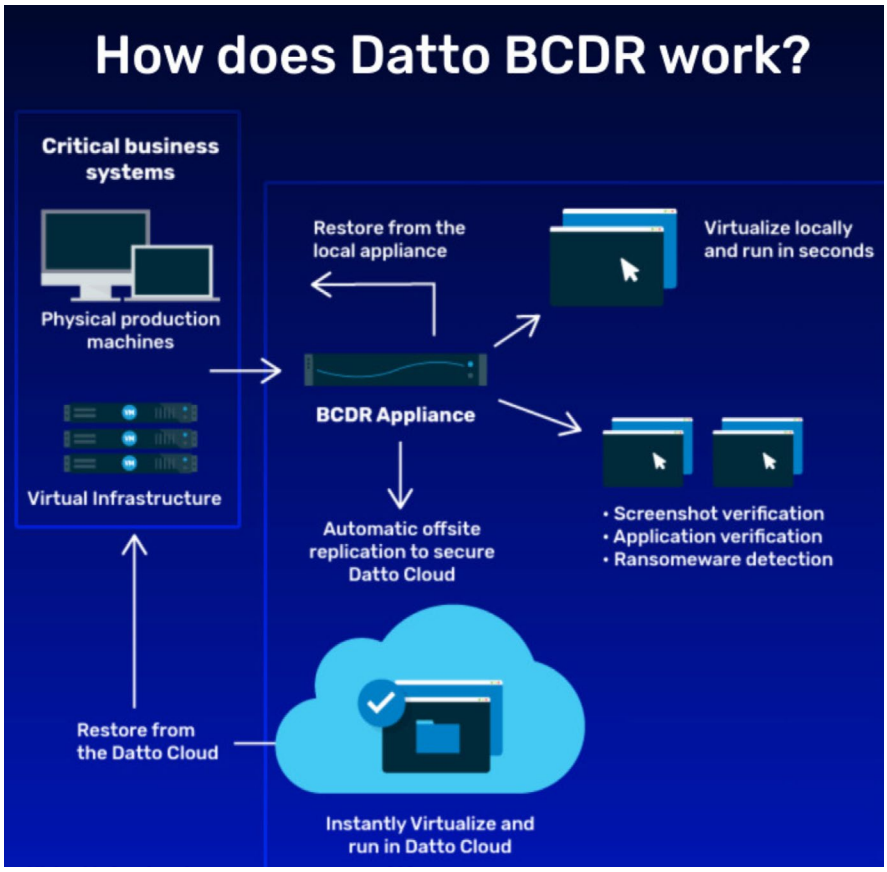
- **Offer tailored BCDR packages**
  Not every client needs the same level of uptime or has the same budget. By offering tiered BCDR packages, MSPs can align service levels with client needs. MSPs can offer basic packages for clients with lower uptime needs and premium packages for those who need instant failover.

- **Bundle BCDR with managed services**
  BCDR is a natural fit alongside core managed services. According to the State of the MSP Industry 2025 Look Ahead report, 83% of MSPs offering co-managed IT already include BCDR due to its critical role in resilience.
  The proven model: Bundle services to drive stronger retention and trust.
  The missed opportunity: Only 46% of MSPs offer BCDR as a standalone service. Elevating it as a core offering can be a key market differentiator.

- **Position BCDR as a business insurance**
  MSPs can shift the conversation by showing clients how a small investment in continuity prevents far greater losses from downtime and compliance failures.
  Break down the true cost of downtime for them: Lost revenue + lost productivity + recovery expenses + cost of intangibles (e.g., reputational damage).
  You can also use Datto's Recovery Time & Downtime Cost Calculator to show exactly how much an outage could cost their business. Try it now.

- **Leverage exclusive MSP programs to maximize profit**
  To get the most from BCDR, MSPs should leverage specialized programs that support sales, pricing and packaging. Datto's Backup Concierge Program is a great example.
  What it provides: A free, dedicated backup solution architect to support every Datto partner.
  What it achieves: Acts as an extension of the team to close more deals and grow profits.

- **Why MSPs trust Datto for guaranteed continuity and resilience**
  For nearly two decades, Datto has been helping MSPs deliver true business continuity. Its enterprise-grade BCDR platform is purpose-built for MSPs, combining powerful technology with ease of management through a single, intuitive portal.



➤ Figure 2: Datto BCDR

What sets Datto apart is its hybrid cloud architecture, offering local backups for fast recovery and automated, hourly replication to the immutable Datto Cloud for disaster resilience. Patented 1-Click Disaster Recovery simplifies failover to a single step, enabling MSPs to meet strict recovery time objectives (RTO) with confidence. With ransomware-proof appliances, role-based access controls and features like Cloud Deletion Defense™, MSPs can ensure their clients stay protected against evolving threats. Automated backup verification adds another layer of reliability, allowing MSPs to prove backup integrity and deliver continuity clients can count on.
Discover why Datto is the BCDR choice MSPs rely on — in their own words.

- *"Datto BCDR has been worth its weight in gold for our business,"* **Aaron Garcia, Director of Operations at TekConcierge**

- *"We've been a Datto partner for 10 years – there is no other organization that offers Datto's level of support,"* **Scott Lennon, CEO of Total Communication**

- *"The client was skeptical that recovery could be achieved without paying the ransom. We stated we were confident it would take nowhere near that time,"* **Linda Kuppersmith, CEO of CMIT Solutions Stamford**

Inspired by how other MSPs are scaling with Datto? You can do it too. For MSPs, BCDR offers a clear path to strengthening client security while unlocking consistent MRR.

Turn business continuity into a competitive advantage. Become a Datto partner today and start delivering the resilience your clients expect — and the profitability your business deserves.

Get started with Datto backup today to maximise MSP profitability and revenue.

MANAGED SERVICES SUMMIT MANCHESTER

18.11.2025

MANCHESTER CENTRAL
MANCHESTER UK

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

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

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

INDUSTRY INSIGHTS

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

NETWORKING OPPORTUNITIES

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

INTERACTIVE EXPERIENCES

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Angel BUSINESS COMMUNICATIONS

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

ITEUROPA

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

https://manchester.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS ITEUROPA ANGEL EVENTS