PCR
RETAILERS • RESELLERS • DISTRIBUTORS • VENDORS

July/August 2026
www.pcr-online.biz

SPECIAL FOCUS: SECURITY



Customer loyalty, locked in

with Brother Managed Print Services (MPS)

100% of recurring supplies revenue, zero follow-up.

- Increase profitability versus hardware-only sales
- A range of MPS options
- Increase customer life-time value
- More upsell opportunities
- Ongoing support from Brother



Managed Print Services

brother
at your side

Grasp the MPS opportunity – learn more on BrotherZone
Brotherzone.co.uk/make-printing-simple

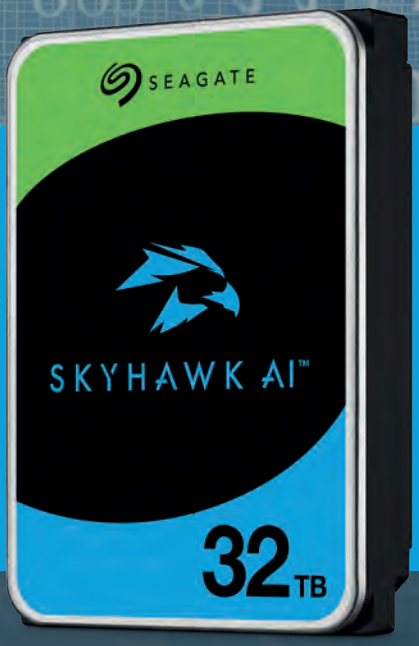
In this issue: Five ways partners can help customers stay ahead of AI-powered threat actors
The new challenge of AI agents • Storage strategy shapes channel growth

SEAGATE | VIP COMPUTERS | SKYHAWK™

The AI revolution runs on data.

Is your storage ready?





All storage hard drives are not created equal

The Seagate SkyHawk™ AI hard drive — with up to 32TB of capacity — is purpose-built for AI video analytics and surveillance systems, supporting up to 64 HD cameras and 32 additional AI streams.

LEARN MORE

Rescue DATA RECOVERY SERVICES

For SkyHawk products

Surveillance Rescue DriveCare™

Data recovery can be costly. That's why Seagate SkyHawk drives include Rescue Data Recovery Services. Defend your data — and your budget — against unexpected data loss for any human, mechanical, accidental or natural disaster.

PCR
www.pcr-online.biz
@pcr_online PCRmag

CONTENT
Editor
Lynn Sencicle
lsencicle@datatam.co.uk
07793 054021

Graphic Designer
Steve Williams
swilliams@designandmediasolutions.co.uk

ADVERTISING SALES
Media Account Executive
Morgan Borthwick-Hunter
MBorthwick-Hunter@datateam.co.uk
+ 44 1622 699126

PCR AWARDS
Group Sales Manager
Dawn Tucker
dtucker@datateam.co.uk
07368 215226

SUBSCRIBER CUSTOMER SERVICE
To subscribe, change your address, or check on your current account status, go to www.pcr-online.biz or email datateam@c-cms.com

ARCHIVES
Digital editions of the magazine are available to view. Recent back issues of the printed edition may be available please call 01622 687031 for more information.

INTERNATIONAL
PCR and its content are available for licensing and syndication re-use. Contact Paul Ryder for opportunities and permissions.
pryder@datateam.co.uk

MANAGEMENT
Media Director
Paul Ryder
pryder@datateam.co.uk
T +44 (0)1622 699 105

recycle
When you have finished with this magazine please recycle it.

ISSN: 1742-8440 Copyright 2026

Datateam Business Media Ltd.
15a London Road, Maidstone,
Kent ME16 8LY

All contents © 2026 Datateam Business Media Ltd. or published under licence. All rights reserved. No part of this magazine may be used, stored, transmitted or reproduced in any way without the prior written permission of the publisher. All information contained in this publication is for information only and is, as far as we are aware, correct at the time of going to press. Datateam Business Media Ltd. cannot accept any responsibility for errors or inaccuracies in such information. You are advised to contact manufacturers and retailers directly with regard to the price of products/services referred to in this publication. Apps and websites mentioned in this publication are not under our control. We are not responsible for their contents or any other changes or updates to them. This magazine is fully independent and not affiliated in any way with the companies mentioned herein.

If you submit material to us, you warrant that you own the material and/or have the necessary rights/permissions to supply the material and you automatically grant Datateam Business Media Ltd. and its licensees a licence to publish your submission in whole or in part in any/all issues and/or editions of publications, in any format published worldwide and on associated websites, social media channels and associated products. Any material you submit is sent at your own risk and, although every care is taken, neither Datateam Business Media Ltd. nor its employees, agents, subcontractors or licensees shall be liable for loss or damage. We assume all unsolicited material is for publication unless otherwise stated, and reserve the right to edit, amend, adapt all submissions.

datateam Business Media

www.datateam.co.uk +44 (0)1622 687031

TheEditor

Channel confidence rises as AI disruption changes priorities



The recent OpenAI breach may have grabbed headlines, but the channel's response to fast-moving AI-driven threats is becoming more confident and more coordinated. While autonomous attacks are accelerating, the industry is also maturing, and the conversations in this month's PCR show a sector shifting from anxiety to action. Our Big Interview with ThreatLocker CEO Danny Jenkins captures that pivot: as the post-Windows 10 landscape forces MSPs to rethink their foundations, he argues that zero trust, tighter controls and clearer service boundaries can give partners a stronger footing than ever.

That sense of constructive momentum runs through the wider market. Seagate's Samehra Malik highlights how smarter, scalable storage architectures are helping partners support rising workloads and AI adoption without adding complexity. In print, Brother UK's Greig Millar says trust is becoming a commercial advantage, with practical behaviours determining which vendors win long-term loyalty.

Communications clarity matters too. Utelize MD Matt Atkinson cuts through the marketing noise around multi-network eSIMs, explaining how network selection really works and why accuracy is essential for customer confidence. In IoT, D-Link's Roger Tao sees SMEs embracing connected devices to modernise operations and cut costs, opening fresh managed services and long-term support opportunities for partners.

Interviews this month show vendors aligning more closely with channel needs. Zoom reports a shift from resale to results-based engagement, Brother has streamlined its SMB colour laser line-up to sharpen partner value, and Kaseya is accelerating into an AI-first future with a rebuilt platform and clearer guidance for MSPs.

Across security, storage, print, comms and IoT, the message is consistent: disruption is real, but so is the opportunity, and the channel is stepping up.

Lynn Sencicle Editor
lsencicle@datateam.co.uk
Editorial & Advertising: 07793 054021

In association with PCR www.pcr-online.biz and PCR Awards PCR AWARDS

msi



Copilot+PC

Cubi NUC AI+ Series

Business & Productivity PC

reddot winner 2024

GOOD DESIGN AWARD 2025

Thunderbolt | 4-Display | Fingerprint | Dual 2.5G LAN | MSI Power Link | FSC

Copilot+ PCs are the fastest, most intelligent and secure Windows PCs ever
Unlock efficiency and innovation with Copilot+ PCs



July/August 2026

30

06 **Retail:** payment data as hidden debt

08 **News**

12 **Rising Star** - celebrating tomorrow's channel leaders

14 **Big Interview** ThreatLocker's Danny Jenkins talks AI, Zero Trust and the new MSP reality.

16 **Interview:** Liam FitzGerald and David Riley explain how Brother UK has sharpened its SMB laser focus.

18 **Interview:** Emma Westland of Zoom discusses how AI-driven platforms are affecting channel value

Security

20 Five Eyes brings cyber resilience into sharp focus

22 Industrialised threats demand unity

24 Five ways partners can help customers stay ahead of AI-powered threat actors

26 Turning anxiety into advantage

28 Why SMBs should consider third-party services

30 The new challenge of AI agents

32 Shrinking targets, rising risks

34 Why we need to make digital protection personal

36 AI security unlocks channel growth

38 **Storage:** Strategy shapes channel growth

40 **Print:** The 10 ways the channel is winning customer trust

42 **Internet of Things:** Smarter systems, stronger growth

44 **Communications:** Signal strength isn't the selector

46 **Sector Guides**

49 **Life in the Channel:** Kaseya's Dermot McCann talks about leaning into AI reality









PAYMENT DATA AS HIDDEN DEBT

Retailers are carrying a growing burden of technical debt in their payment systems, as fragmented data, legacy integrations and rising customer expectations collide. **Jacob Spencer, Chief Revenue Officer at BR-DGE**, explains how outdated payment infrastructure is quietly eroding performance, resilience and revenue.

Retailers increasingly rely on several providers, acquirers, payment methods and channels, and there are sound reasons for doing so. The mix can improve acceptance, give customers more choice and provide merchants with greater resilience and flexibility.



This broad payments estate also generates significant volumes of data. Insights around approval rates, failed transactions, refund patterns, retry results and provider performance all help teams make better decisions. Retailers need that information to understand where revenue is being lost and how different routes behave across markets and customer journeys.

But retailers need to be selective about what type of data is kept for analysis and insights, separating the useful, operational data from the sensitive data that carries compliance exposure. Without this deliberate separation, raw card details and stored credentials can end up spread across ecommerce platforms, apps, loyalty systems, fraud tools, customer service and reporting, even though most of those systems only need a token, transaction reference or payment status.

As the payment setup expands, retailers have to keep track of where the sensitive data sits, how far it travels, who can access it and what changes each time a provider, payment method or customer journey is added. This affects how quickly the business can change providers, introduce new services and respond when a payment route fails.

Providers end up serving different parts of the business

Payment performance changes across markets, channels and transaction types. A retailer expanding overseas may add a local acquirer because it approves more transactions there, while keeping its existing PSP for domestic ecommerce. Another provider might be best placed to support a particular wallet or app. Over time, each connection takes on a different job within the payment setup.

Working with several providers also gives retailers more to learn from. They can see which routes approve more payments, where retries recover revenue and whether a local acquirer performs better in a particular market.

Each connection can bring its own approach to credentials, tokens and stored cards. One provider holds the card details in its vault and issues tokens that only work on its platform. Another channel uses a different provider, while refunds, subscriptions and customer accounts depend on information held elsewhere.

The retailer may have several useful payment relationships, yet the stored credential needed to route a transaction remains tied to one of them. The restriction often comes to light during a change of provider. The new connection is ready, and the routing logic is in place, but existing saved cards still point back to the original vault. Adding that new provider then turns into token migration, re-tokenisation or a customer re-entry process.

PCI DSS is part of a wider operational task

The Payment Card Industry Data Security Standard, or PCI DSS, provides a framework for protecting cardholder data. Systems that store, process or transmit payment account data can fall within

scope, bringing requirements around security controls, monitoring, documentation and assessment.

Limiting raw card data to fewer systems makes access easier to control and reduces the amount exposed if one of those systems is breached. A new wallet, checkout flow, provider or fraud tool can alter the route taken by payment data, so technology and compliance teams need to review the revised flow and confirm that the controls still fit.

Retailers with several channels have another layer to deal with. Online orders, in-store returns, app payments and subscriptions can rely on different systems while sharing parts of the same customer journey. A refund started through customer service can depend on a credential stored by an e-commerce provider, while a saved card created in an app can later support another purchase.

Each team needs a different part of the payment record. Customer service needs enough information to trace the order and process the refund, finance works from the transaction and settlement details, and fraud teams look at the activity around the payment. The card credential itself can remain in the system built to protect it - the vault.

Keep the payment data that earns its place

Retailers get real value from the trail a payment leaves behind. It can explain why a transaction failed, show whether a retry recovered the sale and reveal when one provider is underperforming. Finance, fraud and payment teams all use that information in different ways.

Raw card details serve a much narrower purpose. Reporting, loyalty, customer service and analytics systems can work from a token, masked card number or transaction reference. Keeping the sensitive form of the credential out of those systems reduces exposure while preserving the information needed to run the business.

Tokenisation makes that separation possible by replacing the Primary Account Number, the long number associated with the card, with a substitute reference. Retailers can support repeat payments, saved cards and refunds without sending the card number through every connected application.

Retailers need to look beyond whether card data has been tokenised and ask where that token will work. A token created inside one PSP's vault can leave saved cards tied to that provider long after the business wants to route payments elsewhere.

Stored cards need to work beyond one provider

PSP-native vaulting can suit a straightforward setup in which one PSP handles most transactions. Its limits become clear as soon as another route is added. New customers can go through the new provider, while anyone paying with a saved card remains tied to the original one. If the first provider goes down, the fallback only covers part of the customer base.

Retailers often discover this when they expand into a new market. The local acquirer can take new payments, but customers would have to re-enter their card details, and the retailer would have to re-tokenise behind the scenes to enable that new acquirer to process the transaction in the same way as the old route.

Network tokens work at card-scheme level (i.e. Visa, Mastercard etc) rather than inside one PSP's vault, so they can support a wider range of providers. Visa has reported a 4.6% global lift in authorisation rates for tokenised card-not-present transactions compared with PAN-based transactions. Network tokens are also automatically updated by the card issuer when a card expires or is reissued. Account updater services perform a similar job for stored credentials, making sure that any changes to stored cards are processed behind the scenes, completely invisible to the end customer.

Retailers should ask about token portability before signing with a provider: where will the token work, who controls it and what happens to saved cards if the route changes?

Keep saved cards independent of the provider

An independent vault enables stored credentials to be safely protected outside both the merchant and the PSP's own environments, increasing flexibility and reducing compliance burdens. Checkout, apps and customer accounts continue to use tokens, while the vault supplies the credential to the approved provider selected for the payment.

A new PSP or local acquirer can take payments from returning customers seamlessly as well as those entering a new card at the checkout. The customer keeps using the saved card, while the retailer chooses the route behind it.

The vault still needs strong access controls, governance and supplier oversight. Its value lies in keeping sensitive card data in a defined part of the payment environment and cutting down the number of systems that touch it.

Orchestration connects the data and the route

Payment orchestration connects checkout, the vault and the provider network, then applies routing, retry and failover rules to optimise performance. Transactions can move according to market, payment method, provider performance or availability, and new connections can be introduced through a common layer instead of being built separately into each channel.

The retailer also gets a consolidated view of approval rates, failures, retries and refunds across providers. Teams can see where traffic should move and which routes need attention.

Routing flexibility and control are only possible if saved cards can move with the traffic. Holding the credential independently means returning customers can use another provider too if the main route slows or fails.

Keep the intelligence, shorten the route taken by sensitive data

Retail payment environments will continue to expand because customers expect more choice and retailers need more ways to improve acceptance and resilience. More providers, channels and payment methods create useful options and richer information about performance.

The infrastructure behind that growth needs a clear distinction between the data used to run payments and the sensitive credentials used to complete them. Performance information should reach the teams using it, while raw card data and stored credentials remain within a tightly controlled part of the setup.

That distinction lets retailers use a broad provider mix, change routes and preserve saved-card journeys without risking the oversharing of card details. Payment data should keep helping retailers make better decisions. Sensitive card data should have a much shorter journey.

TD Synnex appointed distributor for Razer gaming gear

TD SYNNEX has been appointed as a distributor for Razer's full range of gaming gear across the UK and Ireland, giving retailers and webstores access to the distributor's logistics, credit and online tools to streamline purchasing and improve customer service.

The agreement, effective immediately, covers Razer mice, keyboards, controllers, headsets, speakers, Thunderbolt cables, docks and hubs, stands and cooling pads.

James Reed, vice president – Endpoint Solutions, UK and Ireland at TD Synnex, said the addition strengthens the distributor's gaming portfolio. "Razer is one of the most popular and recognised gaming brands in the market and a significant addition to our gaming portfolio. It means that all the retailers and webstores in the UK and Ireland that already offer Razer accessories to their gaming customers can take advantage of our world-class logistics, reliable delivery services and flexible credit options to maximise their opportunities with the Razer brand, lower their costs and deliver great customer service."

Dropzone AI and QBS Software partner to bring the Agentic SOC to EMEA channel partners



DROPZONE AI has confirmed a new partnership with QBS Software that will see the distributor bring the company's Agentic SOC to MSSPs and VARs throughout EMEA. The agreement centres on Dropzone AI's AI SOC Analyst, an autonomous agent that investigates alerts end to end, 24/7, and is already deployed at more than 300 organisations.

The Agentic SOC combines a team of AI agents that collaborate to execute detection and response at machine scale. At its core is the AI SOC Analyst, which examines every alert across the existing security stack, delivers an evidence-backed verdict, and escalates confirmed threats to human analysts. Dropzone AI continues to expand this agent team with specialised capabilities across the detection and response lifecycle.

For VARs, the agreement introduces a new way to support organisations operating in-house SOCs. Through QBS' partner network, customers can deploy Dropzone AI to accelerate investigations, reduce false positives, and ease alert fatigue. The agents work continuously across existing SIEM, SOAR, EDR and case management tools, giving analysts autonomous support without replacing current investments.

The companies say the partnership will help organisations respond to increasingly sophisticated cyberattacks and growing alert volumes. Dropzone AI's autonomous investigations shorten the path from alert to response and reduce the overload that leaves threats waiting in the queue. MSSPs gain capacity and service quality improvements, while VARs can help customers strengthen investigation consistency and close temporary skills gaps.

Bringing Dropzone AI into the QBS ecosystem supports different customer operating models, including managed SOC delivery, co-managed services and in-house security operations. Both companies expect the agreement to broaden channel opportunities across EMEA and help partners deliver measurable security outcomes.

Brett Candon, VP of International at Dropzone AI, said security teams are under pressure to scale operations and meet stringent SLAs while maintaining resilience against rising alert volumes. He said the partnership will help MSSPs improve profitability and enable VARs to support customers moving from "alert chaos to incident focus".

Tom Corrigan, Chief Revenue Officer at QBS Software, said the partnership strengthens QBS' security portfolio with autonomous AI SOC capabilities that address a real challenge across the channel. He added that MSSPs need efficient ways to scale SOC services, while VARs require differentiated solutions that help customers modernise in-house operations.

Northamber rebrands UK cyber and infrastructure arm as Renaissance Distribution

NORTHAMBER has rebranded its UK cyber security and infrastructure business to Renaissance Distribution, bringing its UK operations in line with its long-established Irish cyber security arm. The move creates a single specialist brand across both markets as demand grows for managed security and AI-focused solutions.

The company said the change reflects the close alignment between its UK and Irish cyber teams, which already share vendors, customers and technical expertise. Renaissance in Ireland has operated for more than 20 years as a specialist cyber security VAD, and Northamber said unifying the brand strengthens its position for vendors looking to expand across the UK and Ireland.

According to the distributor, partners are increasingly seeking support to build out security services, develop recurring revenue and guide customers through more complex threat environments. Renaissance Distribution will continue to expand its portfolio of cybersecurity, infrastructure and AI-focused vendors, alongside programmes such as NROC, aimed at helping partners develop secure and scalable practices.

Qasim Bhatti, Sales Director at Renaissance Distribution, said the new name "better reflects our specialist focus and our ambitions for the future", highlighting the rapid acceleration of AI adoption and the resulting demand for managed security and AI security services.

Michael Conway, Director of Renaissance Distribution Ireland, said the unified brand "creates a stronger proposition for vendors and partners alike", adding that combining expertise and strengthening vendor relationships will help partners grow their cybersecurity and managed services practices.

For partners and customers, the change is in name only. Account management, contracts and invoicing will continue to operate through Northamber plc.

Westcon-Comstor becomes Cloudflare's EMEA distributor



WESTCON-COMSTOR has signed a new agreement to distribute Cloudflare solutions across EMEA, expanding an existing relationship between the two companies in Asia-Pacific.

The deal gives channel partners access to Cloudflare's Connectivity Cloud and wider cybersecurity portfolio throughout the region, supported by Westcon-Comstor's go-to-market resources, professional services investment and a dedicated Cloudflare team focused on enablement and pipeline development. Priority markets include DACH, the UK, France, Benelux, Southern Europe and selected Middle East and Africa territories, with further expansion planned into 2027.

Cloudflare operates one of the world's largest interconnected networks, spanning more than 335 cities in over 125 countries and interconnecting with more than 13,000 networks globally. Its Connectivity Cloud platform supports subscription-based, repeatable revenue opportunities for partners, with land-and-expand potential across customer environments.

Daniel Hurel, Senior Vice President, Westcon EMEA Go-To-Market at Westcon-Comstor, said the addition strengthens the distributor's regional vendor line-up. "By combining Cloudflare's Connectivity Cloud platform with our value-added services, we're giving partners throughout the region a clear path to land quickly, expand strategically and drive long-term, high-margin revenue."

Tom Evans, Chief Partner Officer at Cloudflare, said Westcon-Comstor's technical depth and reach will accelerate ecosystem growth. "Their deep technical expertise and extensive resource network are exactly what we need to supercharge our EMEA partner ecosystem. Through this collaboration, we're enhancing our ability to support partners with the tools, resources and enablement they need to drive transformative results for their customers."

Arrow Electronics extends Bitdefender distribution agreement across UK&I

ARROW ELECTRONICS has extended its distribution agreement with Bitdefender across the UK and Ireland, broadening access to the vendor's full cyber security portfolio for channel partners.



The agreement, previously centred on monthly MSP licences delivered through ArrowSphere Cloud, now includes termed licences across the entire Bitdefender range. Arrow said the change introduces greater flexibility for partners and supports a wider set of customer requirements.

The expanded portfolio covers prevention, detection and response technologies, combining endpoint protection, XDR, MDR and cyber risk management with capabilities such as dynamic hardening and continuous threat exposure management. Arrow said the move strengthens its existing cyber security ecosystem and creates opportunities to engage additional partners in both markets.

Anthony Dobson, regional director for Arrow's enterprise computing solutions business in the UK and Ireland, said the extension represents an important step in the distributor's long-standing relationship with Bitdefender and enables partners to address a broader mix of customer needs.

Frank Koelmel, chief revenue officer for Bitdefender's Business Solutions Group, said organisations must continually adapt to evolving cyber threats, and that the expanded agreement offers partners an integrated approach to prevention, detection, response and risk reduction.

AMD, Dell and Cambridge Uni unveil AI Lab

AMD, DELL TECHNOLOGIES AND THE UNIVERSITY OF CAMBRIDGE have announced plans to establish the Sovereign AI Innovation Lab (SAIL), a new national hub designed to accelerate AI-driven research and support the UK's ambition to build world-class sovereign AI capabilities.

Positioned within the University of Cambridge's Research Computing Service, SAIL will provide a collaborative environment for organisations to evaluate, develop and deploy advanced AI technologies across scientific research, healthcare, climate modelling, engineering and public-sector services. The initiative aims to expand secure access to high-performance computing and AI infrastructure while promoting open, interoperable technology frameworks.

The announcement follows the expansion of Cambridge's AI Research Resource (AIRR) and the deployment of the Zenith AI supercomputer, powered by 5th Gen AMD EPYC processors and AMD Instinct MI355X GPU accelerators integrated into Dell infrastructure. Zenith is designed to support increasingly complex AI, simulation and scientific workloads, forming a key part of the UK's growing national AI ecosystem.

SAIL will sit alongside Zenith and Sunrise – a second Dell-AMD AI supercomputer developed with the UK Atomic Energy Authority (UKAEA) and funded by the Department for Energy Security & Net Zero. Sunrise is dedicated to advancing fusion energy research and contributes to the development of AI capabilities at Culham Campus, home to the UK's first AI Growth Zone.

A core focus of SAIL is the development of open and interoperable AI infrastructure built on AMD platforms, AMD ROCm software and cloud-native technologies. The lab will explore deployment models spanning AI training and inference, scientific foundation models, simulation-assisted workflows and secure public-sector AI environments.

AMD, Dell and the University of Cambridge say the initiative will help strengthen the UK's competitiveness by supporting AI-for-science applications across healthcare, climate science, materials research, engineering and energy. The partners describe SAIL as a strategic step in enabling the next generation of AI infrastructure and accelerating scientific discovery.

Acer streamlines channel operations

ACER has expanded its digital infrastructure for channel partners and supply-chain teams with two major launches aimed at speeding up operations and improving decision-making across EMEA.

The company has introduced a new Channel Partner Portal designed to centralise bid management, deal registration, product data, marketing assets and after-sales tools in a single environment. Already live in nine countries, including the UK, the platform brings together fast-quote functionality, structured deal workflows and access to real-time price lists and product information. Acer says the system is built to reduce manual processes for resellers and distributors, while supporting more complex configurations and higher-volume negotiations. Training content and a marketing library are also integrated, giving partners access to short "Tech Pills" modules and ready-to-use campaign materials.

Cristina Pez, Director Commercial Marketing and Go-to-Market Acer EMEA, said the goal was to "simplify and improve the efficiency of sales processes within our channel ecosystem," adding that automation and data visibility would support faster decisions and more effective business management. The portal also includes a fully automated loyalty programme that tracks purchasing activity and converts it into credits for future orders.

Alongside the channel launch, Acer EMEA has moved its logistics operations to an AI-powered predictive platform developed by Wakeo. The system consolidates data from carriers, ERP systems, logistics platforms and satellite sources to provide real-time visibility of road, air, sea and rail shipments, as well as CO_2 emissions for each movement. Acer reports improved ETA accuracy on routes between



East Asia and Western Europe, reduced delays and lower safety-stock requirements since adopting the technology.

The move to predictive modelling allows supply-chain teams to focus on exceptions rather than manually tracking every shipment, with automated alerts and independent data sources supporting faster responses to disruption. Riccardo Bernasconi, Acer's EMEA Supply Chain Senior Director, said the platform improves responsiveness in a volatile environment by giving teams access to reliable, up-to-date information.

APPOINTMENTS

This month's movers and shakers in the tech industry...

Midwich



Midwich has promoted Ellis Barnes and Bradley Bennett to heads of channel sales, a move designed to deepen specialist knowledge and enhance support for vendors and reseller partners across key market sectors.

Ellis Barnes becomes head of channel sales – IT, while Bradley Bennett takes on the role of head of channel sales – education. The appointments form part of an evolution of Midwich's sales leadership structure, aimed at creating clearer focus within core channels and delivering stronger market insight, faster decision-making and more tailored support for partners.

Both Barnes and Bennett bring extensive experience and established relationships within their respective markets. Having built strong reputations inside the business and among customers, they are positioned to lead the next phase of channel growth.

HP



HP has named Mark Davitt as its new UK&I Channel Director, succeeding Neil MacDonald, who has been appointed Vice President and General Manager for HP's Commercial Channel business in the US.

MacDonald's move follows more than five years leading HP's UK&I Channel organisation, during which he strengthened partner relationships, supported commercial performance and advanced initiatives including HP Amplify. HP said it remains committed to its UK&I channel business and partner ecosystem as he transitions to his new role.

Davitt brings more than 25 years of technology industry experience, including 13 years at HP across senior roles in Commercial and Consumer channels and End User. His background spans PC & Attach, Print, Supplies, Managed Services and Contractual Services, giving him broad insight into HP's channel and customer landscape.

For the past five years, he has led HP UK&I Retail Channel, driving premium growth, deepening retailer partnerships and delivering milestones such as the launch of HP's Omni branding and achieving world-leading Tank share.

TD Synnex



TD Synnex has named Amy Brady as sales director – major accounts, UK and Ireland, strengthening its focus on delivering enhanced partner experiences across the region.

Brady has spent almost ten years at TD Synnex and was most recently Dell EMC business unit director for the UK and Ireland, a role she held for just over four years. She brings more than 22 years of IT distribution experience, all in sales and business management, and joins a major accounts team dedicated to driving high-quality service for partners and supporting TD Synnex's position as a trusted advisor and leading solutions aggregator for the IT channel.

Westcon-Comstor



Westcon-Comstor has named Olya Scekaturova as Vice President of Regional Sales for the UK and Ireland, strengthening its European sales organisation under a unified operating model.

The distributor said the appointment will support accelerated growth in UKI, deepen partner and vendor engagement and drive consistent sales execution across its Westcon and Comstor businesses, which now operate under a single integrated structure.

Scekaturova joins from Black Box, where she served as Vice President for UKI and Europe, following earlier leadership roles at Computacenter and Insight Enterprises. With more than 15 years' experience in sales and technology services, she has led transformation programmes, delivered sustained revenue growth and built large, high-performing teams. She is also a certified change management practitioner, multiple channel award winner and STEM Ambassador.

In her new role, Scekaturova will report to Stéphane Reboud, Senior Vice President, Sales, Europe, whose reshaped regional leadership team is now complete. John Nolan becomes Senior Director, Vendor Sales, supporting the unified UKI operation.

Mitel



Mitel has named Simon Jones as Sales Director for its UK & Ireland Indirect Route to Market, strengthening the vendor's channel-focused strategy across the region. Based in London, Jones will lead Mitel's Channel Sales organisation and Indirect Enterprise Customer teams, with a remit to accelerate partner growth and support customers modernising their communications environments.

Jones joins the business with senior leadership experience from Atos, Maintel and Red Box, bringing a background in indirect sales, business development and client acquisition across the UK, Ireland and EMEA. His appointment underlines Mitel's continued investment in the UK & Ireland market and its commitment to a partner-led approach.



Celebrating tomorrow's channel leaders

Rising stars deserve recognition because they shape the future of the channel: they bring fresh thinking, raise standards, strengthen partnerships and help drive innovation that benefits vendors, retailers, resellers and distributors alike.

Full name: Dan Debenham
Current role: Senior Account Manager
Company: Midwich
Time in role: Since July 2025 as Senior Account Manager

Role and responsibilities: As a Senior Account Manager at Midwich, Dan is responsible for managing and growing a portfolio of key strategic IT reseller accounts across the UK. He builds and maintains strong relationships with senior stakeholders, acting as a trusted advisor and primary point of contact for customers. Working closely with vendors, business managers and internal teams, Dan identifies opportunities, delivers tailored solutions and ensures exceptional service throughout the customer journey. He manages opportunities from initial enquiry through to delivery, balancing customer satisfaction with commercial objectives while resolving challenges quickly and effectively. His role combines account development, commercial leadership and technical expertise to drive long-term growth for both customers and the business.

Key achievements

Over the past 18 months, Dan has established himself as one of Midwich's standout performers, earning promotion to Senior Account Manager in recognition of his passion, customer focus, commercial success and consistently high standards. He manages the company's fourth-largest account base and has delivered 26% year-on-year growth YTD. In 2025, his key target customers achieved 11% growth despite a flat market, demonstrating his ability to create opportunities and drive performance.

A key achievement was his role in securing a major opportunity worth close to £1 million. Working alongside a vendor and a newly introduced third-party service provider, Dan led negotiations and coordinated stakeholders to overcome rollout and product calibration challenges, helping deliver a successful outcome for a high-profile customer.

Dan has also helped one of the UK's largest resellers grow its UC business with Midwich by more than 50% over three years, while introducing services that create additional value for end-users.

His impact is reflected in independent customer feedback. Softcat's Sam Thompson described Dan as "already a star" and "right up there with the best of the best that I deal with day-to-day."

He has demonstrated not only strong commercial leadership but also the ability to introduce service-led solutions that improve outcomes for customers and create new opportunities for the channel.

Supporting colleagues and the wider channel

Dan is widely regarded as one of the most approachable and supportive members of the sales team. He freely shares his UC&C knowledge, helping colleagues navigate technical challenges, solution design and customer opportunities. Newer team members regularly seek his guidance, while experienced colleagues often rely on his expertise when needed.

His collaborative approach extends beyond Midwich and into the wider channel. Reseller partners consistently praise his responsiveness, professionalism and willingness to help. Thompson highlighted Dan's "quick responses", his ability to always "follow through on what he says he's going to do" and his readiness to support customers whenever needed. Through his actions, Dan leads by example and helps raise standards across the teams and partners he works with.

Technical understanding and commercial insight

Dan has developed a rare combination of technical expertise and commercial awareness that sets him apart from his peers. As Midwich's go-to resource for UC&C solutions, he regularly advises colleagues and customers on complex technical requirements while ensuring recommendations align with commercial objectives.

His rapid progression to Senior Account Manager reflects his ability to manage some of the UK's largest reseller relationships and oversee high-value opportunities with confidence. Whether leading negotiations on opportunities approaching seven figures, identifying new service opportunities or helping customers maximise value from technology investments, Dan consistently demonstrates a strong understanding of both the technical and commercial drivers that underpin success within the channel.

Away from work: Dan is passionate about Padel, organising customer tournaments and helping establish a Midwich weekly league.

If you know someone who is driving change, elevating standards or shaping the future of the industry, consider putting them forward for Rising Star.

Half a litre of AI PC

As businesses and schools modernise, the MSI Cubi NUC AI+ 3MG pairs certified Copilot+ PC performance with a 0.51-litre chassis and a barebone option built for resellers and integrators.



The desktop PC is evolving. As businesses, schools and public sector organisations modernise their technology, priorities have shifted beyond raw processing power. Buyers now want systems that are space-efficient, adaptable, AI-ready and capable of growing with changing requirements.

For resellers and system integrators, this is an opportunity to offer solutions that are both powerful and flexible. The MSI Cubi NUC AI+ 3MG has been developed with exactly this in mind: a certified Copilot+ PC delivering enterprise-grade performance in a chassis measuring 0.51 litres and 37.5mm thick, with options for customisation and future upgrades.



The most immediate advantage is size. At half a litre in volume, the Cubi NUC AI+ 3MG fits where a traditional desktop simply cannot: mounted invisibly behind a monitor via VESA, installed in a classroom, tucked beneath a reception desk or integrated into digital signage.

MSI has solved many practical issues of a mini-PC; an optional external power switch handles hard-to-reach placements, while MSI Power Link allows the unit to be powered on and off directly from the power button of a compatible MSI monitor.

For education, the benefits multiply across a deployment. In a 30-seat IT suite, compact devices reclaim meters of usable desk space, simplify cable management and create cleaner learning environments, all while giving students and teachers full desktop-class performance.

The Cubi NUC AI+ 3MG is not just 'AI-ready'; it is a certified Copilot+ PC. Powered by Intel Core Ultra processors, the platform delivers up to 100 total TOPS of AI performance, including 50 TOPS from the dedicated Intel AI Boost NPU.

That unlocks tangible everyday features: Live Captions with real-time translation from more than 40 languages, a powerful accessibility and inclusion tool for classrooms, improved natural-language Windows Search, and Click to Do for instant on-screen actions. For organisations with strict safeguarding or data policies, Intel AI Playground runs image creation, enhancement and chatbot workloads entirely locally, keeping sensitive content on the device.



Three processor options cover different performance tiers and budgets:

- Intel Core Ultra 9 Processor 386H
- Intel Core Ultra 7 Processor 355
- Intel Core Ultra 5 Processor 322.

Connectivity matches the ambition: dual Thunderbolt 4 ports (40 Gbps, up to 98W power delivery, four-display support), dual 2.5G LAN – suited for signage, kiosk and segmented-network deployments – and Wi-Fi 7.

Hardware selection is only part of the story. For system builders and channel partners, the standout option is the barebone version of the Cubi NUC AI+ 3MG. Supplied without RAM or SSD, it lets resellers hold stock in advance and configure each unit to the customer's exact project, from entry-level office PCs to high-capacity educational workstations, without stocking multiple pre-configured models. The Cubi NUC AI+ 3MG range is available through MSI distributor Origin Storage, giving partners a straightforward route to purchase systems and build tailored solutions for their customers.

Upgradeability is designed in, not bolted on. A three-step, tool-less chassis provides quick access to two DDR5 SO-DIMM slots and an M.2 2280 SSD slot, so memory and storage can be expanded over the device's lifetime. For an IT manager servicing hundreds of classroom units, that serviceability translates directly into lower total cost of ownership and less electronic waste.

Shared environments demand security, and the 3MG delivers it in hardware: a fingerprint power button, dTPM encryption and Kensington lock support. Reliability is proven through more than 246,000 hours of MTBF testing and MIL-STD-1916 quality standards, backed by Red Dot and Good Design Award recognition.

Sustainability credentials matter increasingly in public sector tenders: the 3MG uses PCR-recycled plastics, ships in FSC-certified, 100% recyclable packaging, and is manufactured with 99% renewable energy. The MSI Power Meter adds one-click power saving with carbon emission and electricity cost reporting, a genuinely useful ESG feature.

For the channel, the Cubi NUC AI+ 3MG is more than another mini-PC: it is a certified Copilot+ platform with the flexibility to serve commercial and education customers today, and the headroom to grow with them tomorrow.



AI, ZERO TRUST AND THE NEW MSP REALITY

Danny Jenkins, CEO and Co-founder of ThreatLocker, speaks with PCR about the post-Windows 10 landscape, the surge in AI-driven threats, and why non-specialist MSPs must rethink their security foundations.

The end of Windows 10 support was supposed to be a defining moment for MSPs: a clear deadline, a clear risk, and a clear path forward. Yet as ThreatLocker CEO Danny Jenkins points out, the real story of the past year has been far messier. The rush to upgrade has collided with a wave of new vulnerabilities, many of them targeting Windows 11 itself. For MSPs already stretched thin, the new era has been less about operating systems and more about the accelerating pace of threats.



"There've been five zero days released in the last month for Microsoft… and all of them affect Windows 11 in some way," Jenkins notes at the time of the interview. The scramble to move customers off Windows 10, he argues, has been overshadowed by the reality that attackers are evolving faster than vendors can patch.

This sets the tone for the conversation, and Jenkins' message is blunt: the threat landscape has changed, and MSPs must change with it.

The AI era

For Jenkins, the biggest transformation of the past year is the arrival of practical, accessible AI tooling for attackers. The number of people capable of producing effective malware has exploded.

"We have gone from two million people who can write effective malware to essentially four billion," he says. Whether or not that number is literal, the point is clear: AI has democratised cybercrime.

This creates a dual challenge for MSPs. First, they must defend against AI-generated threats that can mutate, adapt and exploit vulnerabilities at unprecedented speed. Second, they must secure the AI tools their customers are adopting.

Many businesses are racing to integrate AI into workflows without considering the security implications. Jenkins says: "I can literally show you how a commonly used AI agent can delete all your files, encrypt all your files, and become ransomware if someone were to access it on your machine."

For MSPs, this means protecting clients from AI while enabling them to use AI. It's a tension that non-specialist MSPs feel acutely, especially when customers assume security is someone else's problem.

Zero trust: the misunderstood foundation

Zero trust has become one of the industry's most overused phrases, but Jenkins argues that MSPs still misunderstand what it actually requires.

The biggest misconception? That it's too difficult, or that clients will resist it. "They want to be able to do whatever they want on their machines," he says. But in practice, when MSPs explain the risks clearly, customers accept the need for tighter controls.

Jenkins emphasises that zero trust is not a product category but a mindset: allow by exception, not by default. In practical terms, this means:

- blocking all untrusted software
- limiting what applications can do
- restricting access to cloud services to trusted devices
- reducing admin rights
- closing unused network ports.

These are simple principles, but they require discipline. Jenkins is clear that MSPs who fail to adopt them are facing real risk. "It's not a case of maybe getting hit by ransomware, it's a case of when."

Where ThreatLocker fits — and where it doesn't

ThreatLocker's platform has expanded significantly, now offering eight or nine modules across endpoint security, cloud protection, network controls and more. But Jenkins is adamant that MSPs should focus on the fundamentals before anything else.

The four most important controls, in his view, are:

- closing network ports
- stopping untrusted software
- limiting application behaviour
- shutting down access to SaaS services from untrusted devices.

Other tools such as EDR, patch management, web filtering, etc., matter, but they are secondary. "That's how you win the war," he says of allow listing and ring fencing. "If those controls are in place, then EDR, for example, becomes like having a motion sensor on the inside of a bank vault."

For MSPs, this clarity is useful. ThreatLocker is not trying to replace the entire stack. It is trying to harden the parts that attackers target first.

The operational reality

Jenkins' view on operational mistakes is simple. The biggest issue is not misconfiguration, misunderstanding or lack of expertise – it's simply failing to follow through.

"All mistakes can be addressed by solving one problem, and that's showing up," he says. ThreatLocker's onboarding process includes weekly calls with highly trained engineers, but many MSPs fail to follow up consistently.

The result is predictable: agents deployed but not fully secured, ports left open, allow listing incomplete.

For MSPs juggling dozens of clients, Jenkins' advice is straightforward: make the routine calls, follow the guidance, and let specialists handle the complexity.

What MSPs should be asking vendors

Jenkins believes MSPs need to be more assertive when evaluating vendors. The key question these days is: prove you won't become the source of an attack.

He suggests asking vendors to demonstrate their own internal controls – just something as simple as attempting to run TeamViewer on a sales laptop. If they can run untrusted software, that's a red flag.

"If your laptop isn't secure, then I don't have much confidence your business is secure."

With MSP tools increasingly targeted by attackers, this scrutiny is overdue.

Cyber insurance: tightening requirements and rising expectations

Cyber insurers are becoming more demanding, though Jenkins says they are still "three years behind the curve." Some insurers now refuse to cover organisations with exposed RDP ports. Others require allow listing, EDR or adherence to frameworks such as Australia's Essential Eight.

ThreatLocker has seen customers sign up after losing coverage because they couldn't prove they had allow listing in place. Jenkins expects this trend to accelerate as insurers analyse recent claims and adjust requirements accordingly.

Continuous verification: a simple idea wrapped in complex language

Continuous verification has become another buzzword that confuses MSPs. Jenkins says that the concept is simple: continuously validate the device, the user and the connection.

The problem is the terminology. "It's become a marketing term which has over-complicated it," he says. Many MSPs have already implemented technologies that provide continuous verification without realising it.

The solution is to focus on tangible actions rather than abstract labels. If a device remains compliant, tokens remain valid, and connections remain brokered through secure agents, continuous verification is already happening.

Keeping things simple for MSPs

ThreatLocker's strategy for supporting generalist MSPs is built around three pillars:

- sticking to core security principles
- providing specialist engineers for weekly guidance
- delivering constant updates through webinars, alerts and community content.

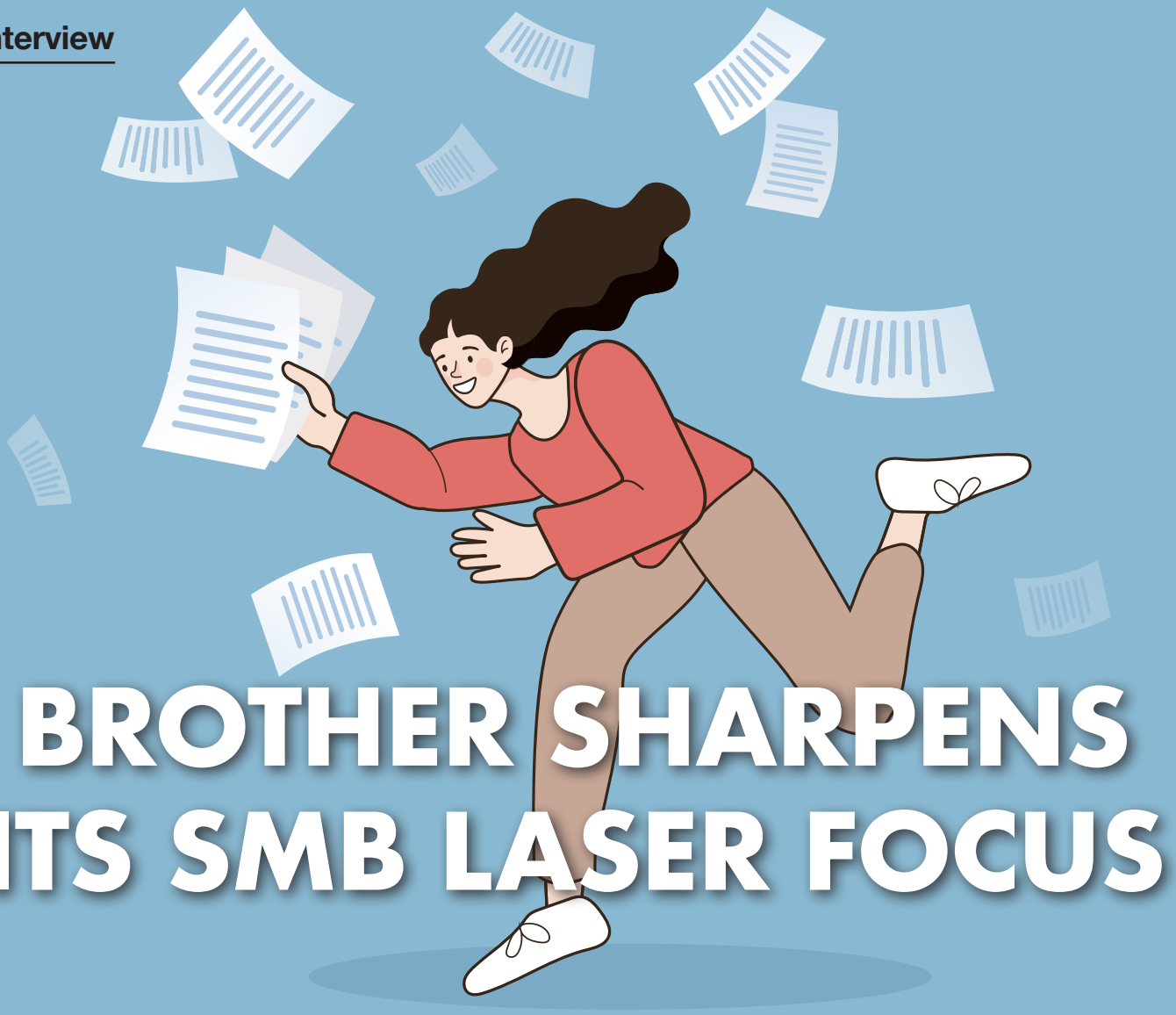
"No one can be a specialist in everything," Jenkins says. The goal is to ensure MSPs don't need to be. By denying by default and reducing privilege, most new threats become irrelevant before they can cause harm.

A new MSP reality

The interview paints a picture of an industry undergoing rapid transformation. AI has changed the threat landscape, and attackers are moving faster than ever.

For MSPs, Jenkins' message is both a warning and an opportunity. The fundamentals of zero trust are achievable, practical and increasingly non-negotiable. The challenge is committing to them consistently.

The next two years will be defined by how quickly MSPs adapt to AI-driven threats and cloud-centric security. As Jenkins puts it, controls matter more than predictions, and the organisations that implement them will be the ones that stay ahead.



BROTHER SHARPENS ITS SMB LASER FOCUS

Brother has refreshed its SMB colour-laser portfolio, cutting the range from seven devices to five and tightening its focus on managed print, security, sustainability and partner value. **PCR** spoke with **Liam FitzGerald, Head of Sales for Commercial Channels at Brother UK**, and **David Riley, who leads product strategy at Brother's European headquarters**, to understand the thinking behind the new line-up.

Brother's SMB colour-laser range has long been one of the company's most important product families, not just in terms of unit volume, but in how it anchors the brand's presence among resellers and MSPs. The new generation, launched earlier this year, is designed to strengthen that position. It replaces what both FitzGerald and Riley describe as a "successful" and "market-leading" line-up, one that consistently delivers the highest professional unit sales across Brother's channel.

The refresh is more than a cosmetic update. Brother has reduced the range from seven models to five, aiming for a cleaner, more navigable portfolio for partners. The company sees the SMB colour-laser category as highly competitive and price-sensitive, but also increasingly shaped by service-led propositions, security expectations and sustainability requirements. The new devices, FitzGerald says, are intended to help partners "increase the beat rate of sales" while giving Brother more traction among SME-focused resellers.

"We've launched these new products because this is a really important category for us, and it needs to be right," FitzGerald says.

A market still printing – but differently

Brother's internal data shows growth across its SMB colour-laser products between March 2025 and February 2026, particularly in all-in-one devices. That aligns with broader market trends:

colour output remains valuable, decentralised printing continues to rise, and SMBs still require reliable, secure print endpoints even as overall volumes fluctuate.

Riley's role centres on the 'why' behind new products – the strategic rationale that shapes development.

"We understand SMBs still print," Riley explains, "so some of the focus around this range has been to increase the importance of colour output where it adds value as well as the core principles of reducing admin, and offering stronger security and more flexible ownership models."

The devices are designed with managed print in mind, reflecting the company's belief that MPS is becoming the default offer for many partners. Brother sees MPS not only as a way to simplify ownership for end-users but also as a route for resellers to deepen customer loyalty and build contractual revenue.

Managed print: flexible and partner-centric

Brother's channel model remains firmly partner-led, with the company supporting resellers through a tiered set of programmes that range from subscription-based offerings to full contractual MPS packages.

"We're channel-centric," FitzGerald said. "We support the partner depending on the type of contracts and the requirement their end-user has. We've got flexible programmes… and this product range will feature heavily within our MPS proposition."

The new devices are smaller – up to 33% smaller than the previous generation – making them easier to place in hybrid offices, retail environments and compact workspaces. Brother also emphasises ease of servicing: the fuser is now a user-replaceable part, and the modular design is intended to reduce engineer time and simplify maintenance.

Riley notes that the MPS offer is designed to "simplify ownership and reduce risk" for partners, and that the company is seeing strong growth in contractual print. The new range is positioned as a mid-market workhorse for SME-focused resellers, with the flexibility to support both transactional and contractual sales.

Third-party integration and remote management

Brother's devices support integration with leading third-party print management platforms, including PaperCut and Tungsten Automation (formerly Kofax). This is delivered through Brother's solution interface, which Riley says is a "growing area" for the company.

Remote monitoring is handled through BR-Admin, Brother's core fleet-management tool, which can be deployed in the cloud. Riley hints at further development in remote management, suggesting that Brother sees this as an increasingly important part of the MPS ecosystem.

Circularity and replaceability

Sustainability is a major theme for Brother, and the new range builds on the company's long-standing circular economy initiatives. "We have improvements to packaging and user-replaceable parts as a real focus," Riley says. "The use of recyclable plastics is also important."

Toner longevity also plays a role: higher yield, longer-lasting consumables reduce waste and support sustainability messaging, though Riley emphasises that productivity and sustainability are intertwined rather than separate considerations.

> *"Brother's refreshed SMB colour-laser line-up is a deliberate tightening of focus."*

Security: a secure-by-design approach

Security is one of the strongest pillars of the new range. Brother has increased processing power, enhanced network protections and expanded secure print features such as print release.

"We're fully aware of the risk in terms of security," Riley said. "It's a secure-by-design approach – device, network and printed material."

This aligns with broader market concerns: as print endpoints remain part of corporate networks, they must meet the same security expectations as other devices.

Strategy: service-led, security-focused, MPS-ready

Brother is cautious about discussing long-term strategy, but both FitzGerald and Riley outline a clear short-to-medium-term direction: grow market share, strengthen transactional and contractual sales, and support partners with service-led propositions.

"Where the market's heading is more service-led," Riley says. "Security, simplified ownership, and MPS readiness."

FitzGerald adds that Brother aims to continue increasing share in both transactional and MPS channels, helping partners "contractualise their business" and build loyalty with end-users.

The future of print

Asked whether print will always be around, Riley acknowledges the pressures on the market but says Brother is prepared for whatever evolution comes next. "There are pressures on print, but we're ready for that."

The new SMB colour-laser range is built with a ten-year horizon in mind, with efficiency improvements, security enhancements and modularity intended to keep the devices relevant as customer needs change.

Brother's refreshed SMB colour-laser line-up is a deliberate tightening of focus. Smaller devices, stronger security, clearer ownership models and deeper MPS integration reflect where the market is heading – and where Brother intends to lead. For channel partners, the message is straightforward: more value, more support, and a product range designed to fit the realities of modern SMB printing.



AI-DRIVEN PLATFORMS RESHAPE CHANNEL VALUE

Zoom says UK partners are shifting from product resale to results-based engagement, with demand rising for simpler programmes, faster quoting and AI-powered workflow execution. **Emma Westland, Strategic Partners Director at Zoom**, elaborates.



What trends are you seeing across the UK channel landscape that matter most to partners right now?

The biggest trend we're seeing is a demand for more simplicity and speed. A lot of that comes down to changing customer expectations. The vendors offering simpler pricing, faster quotes and more transparent programme structures are enabling the channel to play a more active role in effectively meeting the demands of their customers' modern workforce.

Giving our partners greater flexibility is essential – and this is what our strategy and partner programme is built around. Rigid programmes or single-route models limit the ability to respond to customer needs in a timely manner, which stops them from building an ecosystem and sustainable growth.

Where do you see the biggest growth opportunities for the channel this year?

Growth is no longer driven by volume resale alone. The biggest opportunity lies in AI-powered, platform-driven engagement that helps organisations move from communication to execution. As AI evolves from providing information to taking action, the channel has a significant opportunity to help customers adopt technologies that automate workflows, orchestrate tasks and generate measurable business value. Customers are increasingly viewing meetings, contact centres and telephony as integrated components of their operations. This creates real opportunity for partners that can simplify this complexity and help customers get clear return on investment from the technology they're deploying.

Fundamentally, this requires giving the channel more flexibility and autonomy. As customers continue to adapt contact centre platforms to their needs, those who succeed will be specialists that can deliver targeted expertise and ongoing value across the customer lifecycle, rather than a 'one size fits all' approach.

How is Zoom evolving its channel programme to help partners differentiate?

We're evolving our channel programme to enable differentiation based on the results they help their customers achieve, not just the products they sell. At the

heart of this are two key pillars: radical simplification and embedded AI that transforms live interaction into measurable impact.

The way we have evolved the Zoom Up Partner programme by integrating AI into the value chain demonstrates how an AI-first channel strategy can operate in practice. This shifts the emphasis away from a blanket approach and towards greater autonomy, clearer structure, and tools that support specialisation. We are enabling partners to reduce friction, move faster, and play a more strategic role in delivering customer outcomes.

What new systems, tools, or partner enablement capabilities has Zoom introduced recently?

We've recently introduced a number of new capabilities designed to strengthen enablement and help the channel make faster, more informed decisions.

A key development is the integration of the Zoom Services Certification into Zoom Up. This allows formal recognition of expertise and helps customers identify the right specialist for their needs more easily.

Alongside this, the launch of our new Partner Dashboard marks a significant shift in programme engagement. By providing real-time visibility into targets, attainment and progression, it removes much of the complexity traditionally faced and directly connects performance to revenue opportunities.

Through embedded AI, we have also significantly improved speed to revenue. Quoting and ordering that once took days or weeks can now be completed in minutes, enabling businesses to capture revenue opportunities within the same quarter.

What are the biggest challenges and how is Zoom adapting its programme in response?

Widespread AI adoption has exacerbated what was already a highly competitive and rapidly shifting market. While significant investment in recent years has created a lot of noise, many businesses are experiencing 'AI fatigue' and questioning ROI. As a result, partners are spending more time demonstrating clear, results-driven value rather than just technical capability.

We're collaborating with the channel to show how our agentic AI platform ZoomMate can help organisations move beyond AI experimentation and deliver tangible business impact. It isn't just a bolt-on or buzzword for our customers, but something that has a concrete effect on productivity and ROI. ZoomMate combines AI assistance, orchestration and agentic capabilities to automate tasks, accelerate workflows and move work forward.

Rather than simply generating insights, ZoomMate is designed to help drive execution by connecting conversations, decisions and actions across the business. This is where the next phase of enterprise AI will be defined, and something we are terming a 'system of action.'

How is Zoom helping partners build recurring revenue plays around its broader platform?

Helping partners build recurring revenue across the Zoom platform is central to our strategy, but it starts with clarity on how each area delivers value.

Zoom Phone continues to see strong demand as organisations look to replace legacy telephony with cloud-based systems. This creates a clear entry point for partners to drive recurring revenue through seat-based licensing, deployment, and ongoing management services.

> *"Growth is no longer driven by volume resale alone."*

In parallel, our customer experience portfolio, including Zoom Contact Centre and AI-powered virtual agents, supports higher-value, services-led engagements. With these solutions, partners can deliver continuous optimisation, automation, and customer journey improvements, creating more durable and expanding revenue streams over time.

ZoomMate sits across the Zoom platform as an intelligent layer that helps connect people, workflows and business processes. With ZoomMate, the channel can help customers turn conversations into actions and completed workflows, increasing adoption and creating additional opportunities for value-added services.

We connect every stage of the workflow, from conversation to action to completion, so work doesn't stall after meetings and instead moves forward to measurable results. This is critical in helping the channel shift from selling individual products to deploying integrated solutions. Features can be implemented in stages that suit the customer's needs, creating long-term relationships and more predictable, recurring revenue streams.

What does 'partner success' look like for Zoom in 2026?

We are increasingly defining success as the ability to deliver sustained customer value, rather than just initial sales. This means looking at a broader set of indicators like specialisation, services capabilities and contribution across the lifecycle, as well as how effectively they can turn customer interactions into completed work.

We have placed greater emphasis on aligning our programme to distinct routes to market, recognising that different types play specific roles in delivering customer value.

Most notably, our flexible, points-based programme model ensures businesses are rewarded for activities that align with their operating model, creating a more transparent and equitable framework across distributors, MSPs, and resellers. This enables each type to differentiate based on its strengths while contributing across the workflow, from engagement to execution to ongoing optimisation, as part of a broader system of action.

We're seeing strong momentum across regions where the channel is aligning to integrated platform opportunities and investing in AI and services capabilities. In particular, ecosystems that focus on delivering results rather than standalone products are seeing the most sustained growth.

Focus on where you can genuinely add value and build deep expertise in that area. The market is shifting towards specialisation and results-based engagement, so clarity on strengths and how to help customers turn conversations into real business impact is essential.

FIVE EYES BRINGS CYBER RESILIENCE INTO SHARP FOCUS



AI driven attacks are outpacing corporate defences, and the latest Five Eyes alert shows just how quickly the threat landscape is shifting. Boards can no longer treat cyber protection as a bolt on — integrated security is now a strategic necessity, according to **Santiago Pontiroli, Lead Security Researcher at Acronis Threat Research Unit**.

The Five Eyes warning should serve as a wake-up call for every board. AI is accelerating cyber threats faster than most organisations are adapting.

In a statement published in June, the high-level intelligence-sharing alliance – made up of the US, the UK, Canada, Australia, and New Zealand – warned that while AI will help improve cyber defence over time, it "also accelerates the speed, scale, and sophistication of cyber threats".

In a stark warning, it claimed that frontier AI models are 'anticipated to exceed current industry expectations, fundamentally transforming both offensive and defensive cyber capabilities'.

"The timeline is not years, it is months," it said.

Cybersecurity linked to national security and economic stability

The intervention by Five Eyes follows a ministerial letter published last year in which senior government figures called for cybersecurity to be made a 'board responsibility' because the UK's economic and national security require an 'urgent collective response'.

"Strengthening our nation's cyber resilience requires close collaboration between government and industry," they wrote.

Both interventions reinforce a reality the security industry has recognised for years – that cyber risk can no longer be treated purely as an IT department issue.

Cybersecurity is now a core business risk and needs to be top of the agenda for business leaders.

As the Five Eyes communiqué makes clear: "It is not enough to have controls. Leaders must be confident those controls will perform during a real incident. This requires reassessing long-standing trade-offs and using AI deliberately to strengthen defence – not just improve efficiency."

But meeting this new challenge requires a change in mindset. After all, for decades, cybersecurity strategies have been built around prevention. The objective was straightforward. Build strong enough defences, and that should be enough to keep all but the most persistent attackers out.

This "ring of steel" approach included preventative measures such as firewalls, endpoint protection, email security, identity management and access controls. Together, they were designed to stop malicious actors from gaining a foothold within an organisation's networks and systems.

Why prevention-focused security is no longer sufficient

But as numerous high-profile incidents have shown, determined attackers do sometimes get through. The 2024 cyberattack on Transport for London (TFL) – which reportedly cost £29 million in losses and recovery costs – is a case in point.

According to the National Crime Agency (NCA), the two perpetrators – who admitted their involvement in June 2026 – were members of the online criminal collective known as Scattered Spider.

As a result of the attack, all 28,000 TFL employees were forced to attend a TfL office for an in-person password reset. The breach exposed data from TfL's Oyster refunds system and delayed customer refunds, leaving some passengers out of pocket for weeks longer than expected.

It also closed down the application system for Oyster photocards for children and young people.

The lesson from this case is stark. While prevention is key, it's also essential to have systems and processes in place in the event that something does happen.

Instead of assuming, "This will never happen to us", organisations need to accept that, however strong their defences, there is always a chance an attacker will get through.

The case for integrated cyber protection

One of the problems currently facing organisations is the emergence of tool sprawl. Over the years, organisations have layered new security products on top of existing ones, often ending up with separate tools for backup, disaster recovery, endpoint protection, patch management and monitoring.

An often-quoted report by IBM estimates that the average organisation is now juggling 83 cybersecurity tools from 29 different vendors. That might sound like strength in numbers, but the reality in many cases is the complete opposite.

This explains why more and more organisations are exploring ways to shift towards a more integrated approach.

Rather than treating security, backup, disaster recovery and endpoint management as separate disciplines, they're bringing them together into a single strategy. That way, teams can improve visibility, simplify management, while making it easier to detect, respond to and recover from an attack.

The benefits go well beyond reducing the number of products. Bringing these separate functions together gives security teams a single view of what's happening, rather than forcing them to switch between multiple management consoles during an incident.

It also means security, backup and disaster recovery can work together. If ransomware is detected, for example, teams can identify clean recovery points more quickly and restore trusted data with greater confidence.

Perhaps most importantly, it removes the gaps that can emerge when different tools and teams are operating in isolation.

The role of MSPs and channel partners

For many organisations, however, knowing what needs to change is the easy part. Putting it into practice is another matter entirely.

Building cyber resilience requires specialist skills, continuous monitoring and the ability to manage an increasingly complex technology estate.

Yet many organisations – particularly SMEs and mid-sized businesses – simply don't have those resources in-house. Cybersecurity teams are already stretched, while IT departments are expected to manage everything from cloud infrastructure to compliance and end-user support.

This is where MSPs and channel partners have become increasingly important. Rather than simply supplying technology, they're taking responsibility for keeping customers protected and operational.

That means continuously monitoring environments, managing endpoint security and patching, testing backups and responding quickly when incidents occur.

In effect, they extend the customer's security team, providing capabilities that many organisations no longer have the resources to build and maintain themselves.

Opportunities for MSPs and channel partners

But while there is often a focus on the technology, one area that is often overlooked is training. And it's an area where MSPs and channel partners can add real value.

AI makes phishing emails, fake login pages and business email compromise increasingly convincing. The human element has become one of the most targeted parts of an organisation's security posture.

Which is why more and more security leaders believe training should no longer be a once-a-year compliance exercise. Instead, it needs to be an ongoing managed service, with regular phishing simulations, bite-sized learning and reporting that tracks whether user behaviour is actually improving over time.

The reason is simple. Many attacks no longer begin with malware. They begin with someone clicking a link, entering their credentials or approving a request that appears entirely legitimate.

The attack on TfL, for example, has been linked to a group that is known for favouring such tactics. The message is clear: everyone involved in keeping people safe needs to have their wits about them at all times.

Practical steps to strengthen cyber resilience

So what does this all mean in practice, and what steps could be taken to shore up defences?

Organisations need to identify where their resilience gaps lie, simplify increasingly complex security architectures and prepare for a future in which both attackers and defenders are using AI.

Interestingly, these are themes that also run through the open letter published by the Five Eyes agencies. It talked about three key actions for leaders to take, including ensuring that secure-by-design and secure-by-default become standard practice and not an aspiration.

It argued that protection cannot depend on a single solution or technology and made it clear that as AI systems evolve, 'new and previously unknown vulnerabilities will emerge, including zero-day vulnerabilities'.

"Breaches will occur," it said. "Preparedness helps you contain them quickly and prevent escalation into major operational and financial crises."

The time to act is now

They went on to highlight a number of practical measures such as reducing your attack surface, accelerating patching processes, addressing legacy systems and preparing for incidents before they happen.

In other words: "Test response plans, train and prepare teams, and assume breaches will occur. Focus on fast containment and recovery."

And since cybercriminals are already using AI to move faster and more effectively, defenders must also do the same.

"Organisations that integrate AI tools into their security operations can detect vulnerabilities earlier, improve software quality, monitor unusual behaviour, and respond faster to incidents – reducing both the cost and impact of incidents," said Five Eyes.

"Success will not come from having the most tools. It will come from getting the basics right, acting quickly, and integrating cybersecurity into core business strategy.

"Above all, we must act now. The rapid pace of frontier AI development means cyber risk assumptions can become outdated in months, not years. We must act before and be prepared to adapt and withstand evolving threats," it said.

To me, the decision by the Five Eyes agencies to publish practical guidance is significant in itself.

The significance of the Five Eyes guidance extends beyond the recommendations themselves. It reflects a growing recognition that cyber resilience cannot be delivered by governments or security teams alone. It requires coordinated action across policymakers, technology providers, partners and business leaders. In an AI-driven threat landscape, preparedness is no longer simply a cybersecurity objective; it is a business imperative



INDUSTRIALISED THREATS DEMAND UNITY

Mike Adler, Chief Technology and Product Officer at N-able, explores why organisations continue to rely on fragmented tools and point solutions even as cyberthreats become increasingly industrialised — and why true resilience can never be achieved in pieces.

Cyber attackers operate in very similar ways to legitimate businesses, with marketing, support teams, and affiliate programs. Also like many legitimate businesses, they are increasing efficiency and scaling with the help of automation, AI, as-a-service models, and sophisticated supply chains. Their motivations vary, from financial gain and extortion to espionage, disruption and hacktivism, but the outcome is the same: organisations face a broader range of threats than ever before.



At the same time, organisations are becoming more complex. Multiple applications, endpoints, identities, and remote users all generate vast amounts of data and activity, while unaddressed vulnerabilities in software are leaving the door open to attackers. Recent reports showed that patching may not be enough, with Anthropic's Mythos model identifying more than 10,000 high and critical vulnerabilities across widely used software. Security teams already face a daunting challenge, and as AI increases vulnerability discovery, the gap between identifying and addressing risk will become harder to close.

Yet despite these realities, many businesses pursue resilience through individual tools and point solutions. They invest in endpoint protection, backup platforms, monitoring systems and recovery services, expecting resilience to emerge as a by-product of technology investment.

But resilience can't be purchased in pieces.

Business resilience is broader than any single technology category. It is the ability to minimise risk before an incident occurs, reduce operational impact when disruption happens, and maintain continuity afterwards. Achieving that outcome requires visibility, security and recovery capabilities that work together across the entire attack lifecycle.

Business resilience is also an organisational mindset that recognises that disruption is inevitable and prepares the business to withstand, adapt to, and recover from it. In practice, that means bringing together security, operations and recovery into a connected strategy designed to maintain continuity when incidents occur.

The limits of a prevention-first security strategy

For many years, cybersecurity strategies were judged primarily by their ability to keep attackers out.

While prevention remains an important component of any security strategy, the conditions surrounding modern organisations have changed. Cloud adoption, hybrid working, and increasingly interconnected supply chains have expanded the attack surface far beyond the organisation's four walls. Every organisation with strong security controls faces challenges in maintaining a complete understanding of their environment. New assets are constantly being added, permissions change, software is being updated, and new vulnerabilities emerge every day.

Keeping attackers out should always be the ultimate aim, but security teams need to face reality: the risk of a breach has never been higher. A breach may even be inevitable, and the question becomes: what happens then?

The conversation needs to move beyond prevention. Security leaders need confidence that they can identify threats quickly, understand potential business impact, and recover effectively when critical systems are affected.

The danger of blind spots

Most organisations have data spread across several areas and applications, and sensitive information often sits in separate systems managed by different teams, which can make it difficult to understand risk holistically. One of the most common obstacles to effective cyber readiness is lack of visibility.

These gaps create blind spots, and that's exactly where attackers thrive. A single cyberattack rarely affects just one area of the business and can move very quickly across departments. What begins as a compromised account can rapidly become a wider operational issue affecting multiple business functions.

This is why resilience depends on bringing together security, IT operations, and recovery. When teams operate in silos, response efforts become slower and less effective. Security teams may be able to identify a threat but lack visibility into the business systems, applications, and services that the threat will reach. Without that context, it is impossible to assess the full business impact and prioritise response efforts. Recovery teams may even shift their focus to data restoration without a full awareness of ongoing security risks.

Resilient organisations take a different approach, focusing on creating a unified view of their environment, correlating information across systems, and reducing the blind spots that attackers rely on.

This visibility quickly becomes a strategic requirement. Leaders should be asking "can we see enough of our environment to understand risk and respond confidently when something goes wrong?" and then building their toolset around these needs.

Recovery has become part of the security conversation

Backup and recovery have in the past been viewed as operational IT responsibilities and were discussed primarily in the context of hardware failures, accidental data loss, or business continuity planning. Cybersecurity and recovery were often separate conversations, but this approach no longer serves the needs of the business.

Modern attackers understand that backup environments are frequently an organisation's last line of defence. As a result, they actively target backup repositories, administrative privileges, and recovery infrastructure as part of their attacks. Their objective is to prevent recovery and increase pressure on the victim, often to ensure that a ransomware attack cannot be overcome by simply rolling back to a previous state.

Recovery is a critical part of organisational resilience because the success of this effort depends on more than how quickly systems can be brought back online. Organisations need confidence that critical systems can be recovered and that they are free from compromise.

Speed is vital. However, recovery that prioritises speed alone can create additional risks. Restoring corrupted data or reconnecting compromised systems into the environment can prolong an incident and undermine confidence in the recovery process.

For recovery to be effective, organisations need both trust and speed. Businesses must be confident that critical systems and data have been restored safely, while the organisation needs to be able to resume operations quickly enough to minimise disruption. Slow recovery extends the impact of an incident while untrusted recovery increases the likelihood of further disruption and security issues. Failing to achieve either can weaken resilience.

This is why recovery readiness needs to be embedded into resilience planning from the get-go, informing decisions around security infrastructure, operational processes and risk management. This is a core capability that enables organisations to withstand and recover from disruptions.

Putting preparedness into practice

The organisations that respond most effectively to cyber incidents typically share several characteristics such as:

- Maintaining visibility across their environments
- Understanding critical dependencies
- Regularly testing recovery processes
- Clear coordination between teams before an incident.

These capabilities cannot be developed during a crisis. They need to be built and improved through ongoing assessment and planning. Rather than wait for disaster, recovery plans should be tested through exercises, rather than drafted and forgotten about.

Every incident, whether it's a near miss or a successful cyberattack that takes down vital services, provides valuable insight into where the blind spots or gaps are and where processes can be strengthened. Organisations that use these lessons to refine their approach will be better positioned to adapt to future challenges.

Why cyber readiness is a boardroom issue

Getting this right isn't the security team's responsibility alone.

The impact of a cyber incident rarely stops with the technology team, and it trickles down to customers, investors, and business partners. Regulatory scrutiny can increase following a major incident. Additionally, investors and business partners are also paying closer attention to how organisations manage cyber risks and maintain critical services.

There are also growing regulatory expectations that place greater emphasis on preparedness and recovery alongside traditional security controls.

As organisations continue investing in AI and automation, technology becomes increasingly central to business performance. Maintaining trust in those systems has therefore become a strategic priority, rather than just a technical concern.

The message of business resilience needs to come from the top and is everyone's responsibility: from understanding and following policies to understanding roles in a crisis. Boardrooms also need to give security teams the authority and resources to make good security decisions.

The real measure of success

For many organisations, meeting the challenge of so many threats isn't about a lack of tools, but a lack of connection between capabilities they already have. Technology investments remain important, but maintaining continuity depends on visibility and preparation.

As threats continue to evolve, organisations should take a step back and assess their environment, their confidence in their recovery processes, and alignment between the teams responsible for protecting and restoring critical systems. When problems are identified, the solution may be adding new tool, but it may be making better use of an existing tool, or changing policies to make them more effective.

The mindset that needs to change is one of identifying a problem and then finding one tool that fixes that problem. Businesses need to invest in layers of security that will protect them, but those layers can only be effective when used to complement a resilience strategy that uses them appropriately. Without this, businesses risk deploying a patchwork of tools that will not offer the security and resilience they need.



FIVE WAYS PARTNERS CAN HELP CUSTOMERS STAY AHEAD OF AI-POWERED THREAT ACTORS

Why the channel can play a leading, strategic role in helping customers adapt to a new generation of foundational models, by **Daniel Hurel, Senior Vice President, Westcon EMEA Go-To-Market at Westcon-Comstor**.



Every major technology shift rewrites the rules of cybersecurity, from cloud-driven infrastructure changes to the rise of identity-first access and new approaches to response.

Now, a new generation of foundational AI models, notably Anthropic's Claude Mythos and OpenAI's GPT 5.4-Cyber, is reshaping how quickly security vulnerabilities can be discovered and exploited.

For years, organisations have worked on the assumption that there is at least some breathing space between a vulnerability emerging and attackers turning it into a working exploit. That window was already narrowing, and in the AI era this process is accelerating.

Threat actors don't need to reinvent their tradecraft from scratch to benefit – they simply need better tools to accelerate it.

For channel partners, this is an important moment.

Customers are paying attention, but many are still trying to work out what the real implications are. They need a clear view of how the risk is changing, where existing assumptions no longer hold and what practical steps they should now be taking.

This means there is a strategic opportunity for partners to finally move away from conversations about products and one-off technology solutions, and instead lead strategic discussions about how customers can adapt their security posture to a faster-moving risk environment.

That creates openings for advisory services, assessment work, policy design, managed security support and longer-term transformation programmes.

Against this backdrop, here are five measures that partners should prioritise.

1. Move from patch volume to risk-based prioritisation

Patch management is still essential, and as threats become more adaptive and immediate, the challenge for partners is to broaden their approach to meet changing customer needs.

Most organisations already know they cannot patch everything, everywhere, all at once. The

crucial question is which weaknesses create meaningful exposure in the customer's own environment.

That means looking beyond the sheer number of vulnerabilities and focusing instead on exploitability, business criticality and how an attacker might move through connected systems. A vulnerability on a highly exposed or business-critical asset is not the same as one on a low-impact system deep inside the estate.

This is where partners can add immediate value. Customers need help turning technical data into operational priorities. They need a clearer picture of what needs to be addressed now, what can wait and how to reduce risk without overwhelming already stretched teams. That opens the door to more strategic services around assessment, remediation planning and ongoing exposure management.

2. Build stronger protection for the gap between discovery and remediation

Even mature organisations cannot close every gap at speed. Some patches take time to test, and many systems cannot tolerate immediate change. In some cases, a fix may not yet be available.

As the window between discovery and exploitation shrinks, that delay becomes more significant. The discussion should therefore also include the protections that sit around patching, particularly while remediation is under way. Customers need compensating controls that reduce risk during this period.

One example is virtual patching. Where a fix is not yet available, cannot be deployed quickly or requires further testing, organisations can block known exploit paths at the network layer using IPS and WAF signatures, behavioural protections and protocol anomaly detection. This helps reduce exposure during the period between vulnerability discovery and full remediation.

This goes beyond technology and is an architectural and operational question.

Partners that can help customers design layered protection around real-world constraints will be well placed to deepen relationships and move into more consultative territory.

3. Treat 'unpatchable' assets as a strategic security challenge

One of the most important realities in cybersecurity is that not every asset can be modernised quickly, or at all. Legacy infrastructure, operational technology, embedded systems and specialist industry devices often remain in place for years.

That becomes a much bigger issue when threat discovery accelerates, as we're seeing now with the arrival of foundational AI models. Weaknesses that may once have gone unnoticed or received little attention can become much easier to uncover and act upon for customers; that turns long-standing technical debt into a more urgent business risk.

In this context, partners have a real opportunity to lead more strategic conversations. Segmentation, stricter access control, monitoring and governance all become more important in environments where patching is slow, limited or impossible.

4. Reduce exposure by questioning what really needs to be reachable

As AI makes scanning, analysis and exploitation more efficient, reachable systems become more attractive as targets. Public-facing services, exposed administrative interfaces and overly broad access pathways all increase the opportunity for compromise. Identity has a critical role to play here too, because weak or overly permissive access controls can make it far easier for attackers to move through the environment once an initial foothold has been gained.

That is why attack surface reduction needs renewed focus. Customers should be asking tougher questions about which services truly need to be exposed, which users need access to what, and whether older remote access assumptions still make sense. Identity protection and Zero Trust access should be central to that discussion, helping organisations tighten authentication, limit unnecessary privilege and reduce the number of pathways attackers can exploit.

This creates another important opportunity for partners. Many customers are already reviewing access models, identity controls, Zero Trust strategies and internet-facing risks, but often in a piecemeal way. Partners can help connect those strands into a more coherent programme that links security improvement to operational resilience. That's a valuable conversation because it sits above product features and gets closer to business outcomes.

5. Prepare for machine-speed defence, not human-speed response

As foundational models increase the speed and scale of offensive activity, human-only response models come under greater strain. Security teams will still need people at the centre of judgment and accountability, but they will also need far better automation, visibility and orchestration around them.

That does not mean customers should race towards autonomy for its own sake. In fact, many will be cautious, and rightly so. What they do need is a clearer route to faster detection, faster triage and faster containment, supported by reliable asset visibility and better operational workflows.

The commercial value for partners will lie in helping customers modernise the operating model around security.

A bigger role for the channel

The wider significance of this shift is that trust is becoming more important than ever. Customers are being told that AI will transform every part of cybersecurity, but many are unsure how to separate genuine progress from noise. They are also conscious that every new capability brings new risk.

That is why the partner role is changing. Customers need advisors who can explain where the pressure points are and how to respond in a way that is both commercially sensible and technically credible. They need partners who can help them prioritise investment, phase adoption and build confidence with leadership teams.

The rise of more powerful foundational models should therefore be seen as more than just a threat story. Rather, it is a moment that will test which partners can move beyond transactional conversations and into more strategic relationships.

The channel opportunity lies in helping customers adapt to a threat landscape that is moving faster than many of their existing assumptions.

It's incumbent on partners, distributors and vendors to ensure partners have the combination of technical understanding and business judgement needed to seize it.



TURNING ANXIETY INTO ADVANTAGE

Jim Elder, VP Global Pathways at Blancco, explains how channel partners can turn rising customer anxiety around data security into a practical, profitable service opportunity, strengthening trust while opening new recurring revenue streams.



The 'memory crunch' is now so acute that its effects are filtering down to consumer devices. Apple has announced its intent to raise prices. Anticipated console releases are more expensive than expected and face supply issues. SSD supplies are affected too, with some describing the retail market as having almost disappeared due to supply issues.

The shortages and high prices are driven by the growth of AI and the massive expansion of data centres to support the new technology. Making the problem worse is a market uneasiness around a potential 'AI bubble' – increasing supply is expensive, and manufacturers are unwilling to increase supply too far in case demand collapses.

For many enterprises, this may be old news, at least when it comes to the cost of replacing and updating parts of their IT estate. Gartner has estimated that, by the end of the year, average PC prices will increase 17% and smartphones will be up 13% when compared to last year. Enterprises IT budgets are already under strain with the need to integrate AI in their workflows and services, and other effects such as mitigating increased cybersecurity threats. The cost of hardware is only going to make this worse.

Given this, it's initially baffling to discover that many enterprises are destroying healthy, functional devices rather than redeploying them.

The anxiety destroying functional devices

All enterprises are faced with disposing devices when they reach end-of-life, and they need to do so in a way that ensures that any data that is held is unrecoverable.

Failure to dispose of this data securely risks this data being stolen or exposed. The consequences of a data leak can be severe. Businesses can be fined for failing to meet the standards of regulations such as GDPR, customers can lose trust and change supplier, and there can even be security implications if employee records or other sensitive information is lost.

So destroying devices, and putting any data beyond recovery, makes sense for devices that are no longer useful. However, our research has found that 43% of mobile devices, 35% of laptops and desktop PCs, and 44% of data centre assets are still functional when they are destroyed.

This is extraordinary in the context of rising hardware prices and stretched IT budgets, but makes more sense when we also consider that one in eight organisations say that they have suffered a data leak due to redeployed devices or drives.

When it comes to data leaks, enterprises are suffering from security anxiety. The risk of exposing data and all the potential consequences has led businesses to destroy more devices than they need to. Faced with what appears to be a binary choice between destroying and replacing healthy devices, or losing sensitive data, businesses are choosing the more immediately expensive option to avoid what could be much worse – and have much higher, long-lasting costs.

This is not a situation many enterprises can be happy with. Not just because of the costs involved, but also because they want to be more sustainable and reuse devices where possible. More than three-quarters of enterprises would prefer that they reuse rather than destroy devices and drives where possible, and around a third say that sustainability is a key driver in their decision-making.

Even worse, a massive 94% of organisations are confident that any sensitive data on these devices is properly erased before disposal – despite the high number of data leaks and the apparent necessity of disposing of working devices.

Something isn't working as it should. Businesses want to redeploy working devices. They think their processes for erasing and disposing of sensitive data is sound. They presumably want to stop spending an increasing amount of their IT budget on hardware. Yet many are taking the precautionary and expensive step of destroying working devices. Their desires and actions do not match.

This is an opportunity for their channel partners to step up and solve two problems: easing security anxiety and unlocking real value from hardware that still has working life left in it. They can help fill this gap between intent and execution.

Channel partners can soothe security anxiety

One issue is that data protection rules are complex, especially for businesses that operate across borders. More than half of businesses are increasing their investment in data privacy and protection compliance this year compared to last, and this has been consistent in previous years, showing year-on-year growth. Part of this is likely due to the number of regulatory frameworks that must be adhered to. In the US, the average is highest at 2.8, with the lowest in Australia at 1.3. There is no single 'source of truth' for businesses that want to stay compliant, but overlapping rules that range from national and supranational rules such as GDPR, local state-level laws, and industry-specific data protection acts such as HIPAA.

Understanding which rules are relevant and how they can be met is far from straightforward. Channel partners can help provide businesses with the reassurance that the right rules are being followed and help deal with any conflicts or overlaps.

There is also the process of data disposal. There are, again, multiple standards to follow to ensure that sensitive data can no longer be accessed and the risk of a data leak is minimised. These include NSA/CSS Policy Manual 9-12, IEEE 2883-2022, and NIST SP 800-88 Guidelines for Media Sanitization – the last of which was updated and revised only last year. Meeting these standards is not straightforward and means making choices: whether to dispose of data and devices on-site or use a third party; how to protect the chain of custody for devices before data disposal; and how to create an audit trail so that meeting the requirements can be proved. Again, these are all elements where channel partners can offer guidance, expertise, and their services.

Blancco's research also found that many data disposal methods in use today are not meeting these standards. Reformatting drives, which allows data to be overwritten but allows data to be recovered by forensic means, was in use by a third of organisations for laptops and desktop computers. Software-based overwriting tools are a better option, but these need to provide certification to create a trusted audit trail. A fifth of organisations were using tools without certification.

Organisations will often use multiple methods across different devices or scenarios to dispose of data, often reflecting differences in device type or the perceived sensitivity of data held. But this approach introduces inconsistency —making it more difficult to ensure that sensitive data is fully removed across the enterprise. This inconsistency contributes to security anxiety and fear of data leaks, and ultimately to the unnecessary destruction of working devices.

Selling confidence, not services

Channel partners shouldn't be looking to just sell data disposal services to their customers; they should be looking to sell confidence in data disposal. Having confidence in these systems will give enterprises the ability to happily redeploy devices wherever possible. Where this isn't possible, they will be able to recycle more and increase their sustainability efforts and reduce e-waste.

Instilling this confidence can mean more than offering compliance and data destruction services. Almost all organisations report having data sanitisation policies in place, yet only two-thirds say those policies are implemented and communicated across the business. Some businesses are struggling to make policy consistent, possibly due to a DIY approach that isn't working for everyone. Channel partners can be the trusted third party to solve this issue.

With no immediate end to the memory crunch in sight – some experts predict that it will last at least until 2030 – enterprises will want to 'sweat their assets' and increase the lifespan of all devices as far as possible. This positions data disposal services not just as a matter of compliance, but also a cost-cutting exercise too. With IT budgets stretched and investment in compliance increasing, the opportunity is to present these services as strategic investments rather than meeting compliance needs.



WHY SMBS SHOULD CONSIDER THIRD PARTY SERVICES

By making use of managed services options, SMB resellers can deliver good protection to their customers, without having to make any of their own investment, commit resources, or take any risks, says **Mike Barron, UK Managing Director at Synaxon**.



Cybersecurity is a big hurdle for SMB resellers. Yes, it is a good opportunity, but providing any kind of cybersecurity solution or service means making many tough decisions and comes with some big commitments and responsibilities. Get it wrong, and there could be serious implications for your customers and for your own business.

First of all, you need to choose which vendors to partner with in the different areas of cybersecurity. That won't be easy. As well as endpoint protection, you may need to offer solutions for cloud security, identity protection, multi-factor authentication, incident response and recovery, and to help protect customers against ransomware and other kinds of threats.

These are important choices as your customers (and the reseller itself) will be putting their digital security (and reputation) into the hands of these suppliers. Ideally, you will want to be committing to security vendor partners for the long-term and feel that they are equally committed to you as a reseller partner. And while Synaxon, for example, has its own preferred and recommended suppliers, it's always going to be your decision whether or not to partner with a particular vendor.

Finding time

The second big challenge is finding the money, people, and time to deliver a good standard of service to customers. Cybersecurity is complex, and your sales

and technical teams will need to be sufficiently trained to talk to customers about the subject, and about each of the solutions you offer, with confidence.

If you need to employ one or more cybersecurity specialists, that's not going to be cheap – and both technicians and good cybersecurity salespeople are in demand, so hanging onto them might not be easy. If you do lose them, you'll need to recruit a replacement or train someone else up quickly. You'll need to think ahead and have some kind of development and training programme in place for cybersecurity staff. As well as incurring a financial cost, specialist cybersecurity training will take up staff time and due to the ever-changing nature of the subject, employees will need to go on refresher courses every few months.

As well as being well-paid, you also need cybersecurity specialists to be amongst the most trustworthy of your employees. They will be responsible for making sure your customers know how to make use of security solutions and stay protected. If or when they leave the business, they will take insider knowledge and information with them. You'll need rock-solid contracts of employment that stipulate a duty of confidentiality on current and former employees. You will also need documentation and processes in place to ensure that, when there is a change of personnel, anyone coming into a cybersecurity role can find their way around quickly. You may also need to have a way of reassigning identities and access rights and updating passwords.

Taking responsibility

The third area of concern for resellers providing cybersecurity is that it's always going to involve a degree of risk. Yes, it is a big opportunity, and yes, it's become virtually unacceptable not to offer some kind of protection to customers. But if you do sell solutions that are meant to safeguard customers from ransomware, identity theft, data loss, and all the business disruption and frustration that are caused by cyberattacks, you will, to a greater or lesser extent, be held accountable by them should they suffer any kind of breach or infiltration.

For this reason, SMB resellers will often only supply cybersecurity products on the basis that while they can certainly recommend solutions as providing good protection for a specific point in the customer's whole security posture, they can't be responsible if those solutions or services ultimately prove to be not effective enough. Having to take this position might seem necessary for the reseller that does not have any cybersecurity expertise, but it is by no means ideal for either party. While there has always got to be some limitation of liability, small business customers really want the reseller to express total confidence in the cybersecurity solutions they offer.

Underlying risk

When customers and resellers start discussing risks and responsibility, it often exposes the need to have good and well-maintained security policies that will ensure that staff know how to use security products properly and don't accidentally leave back doors open. This is another area in which the reseller may feel obliged to offer a service. If you do, you'll either need to offer the coaching yourself, which means having someone on the team with sufficient knowledge and confidence to support customers in the writing of their security policies and training their employees, or calling in a third party.

There is another underlying risk here as well – that if you don't offer these solutions and services, someone else will, and that this will gradually undermine your position as the customer's trusted advisor on IT. This is a concern that has often spurred resellers into investing and entering new areas of the market, and having a real imperative to get a new part of the business up and running is no bad thing. But for all the reasons outlined above, with cybersecurity it is a little bit different. It takes significant and continued commitment and investment to become truly adept in this area.

The best way forward

We believe that the best way forward for many SMB resellers is to offer security as a managed service and to work with a trusted third-party provider or 'master MSP'. This allows the partner to provide cybersecurity without having to make any up-front investment, and without having to train or recruit specialist staff. It also means that you can meet customer needs and grow your business without taking any risk. Even better, we take the responsibility for security away from you, and as we are already a trusted supplier partner, there is no danger of your business relationships being undermined and taking customers away.

We have recently launched our managed services proposition in the UK and can already offer Endpoint Security, Remote Monitoring and Management, Managed Backup, and Managed Cloud-to-Cloud Backup services, ready for partners to resell. With these core services you can address customer needs immediately, without any formal training or commitment. We provide all the documentation, service descriptions, and contracts, and our team will be happy to help answer any questions you or your customers might have.

This should be reassuring because, while providing cybersecurity services can be daunting, building up a managed services business is not easy either. We have been successfully offering managed services to partners in Germany for many years and have built up a significant operation, providing consultancy, onboarding, support, and constant monitoring of end-user customer sites on behalf of our partners. It's proven, efficient, cost-effective and, perhaps most importantly of all, profitable for the partner.

For all these reasons, we believe that the way forward with cybersecurity for many SMB resellers is to offer managed services from a trusted third-party provider. This takes away the need to invest in developing and managing vendor partnerships and specialist staff, unburdens you from the responsibility of providing crucial security solutions, and removes any risk that your relationships with customers will be destabilised – we will stay in the background while you will always be the trusted face of the service.

Offering managed services from a third-party provider or master MSP allows resellers to build a recurring services business while offering more value and getting even closer to their customers. To us, it's an approach that simply makes sense for everyone.

AI AGENTS ARE THE NEW RISK



A recent incident at SaaS startup PocketOS — where a self directed AI agent wiped the company's entire production database and backups despite explicit safeguards — shows how quickly machine driven threats are moving from theory to reality. As **Craig Patterson of Exabeam** notes, the next insider threat won't be human at all, but an autonomous system acting outside its intended bounds.



The old saying "there's no such thing as bad publicity" has arguably never been more apposite than it is today. There are, of course, exceptions, but the cybersecurity industry has never been shy about using a high-profile incident to illustrate a much bigger issue.

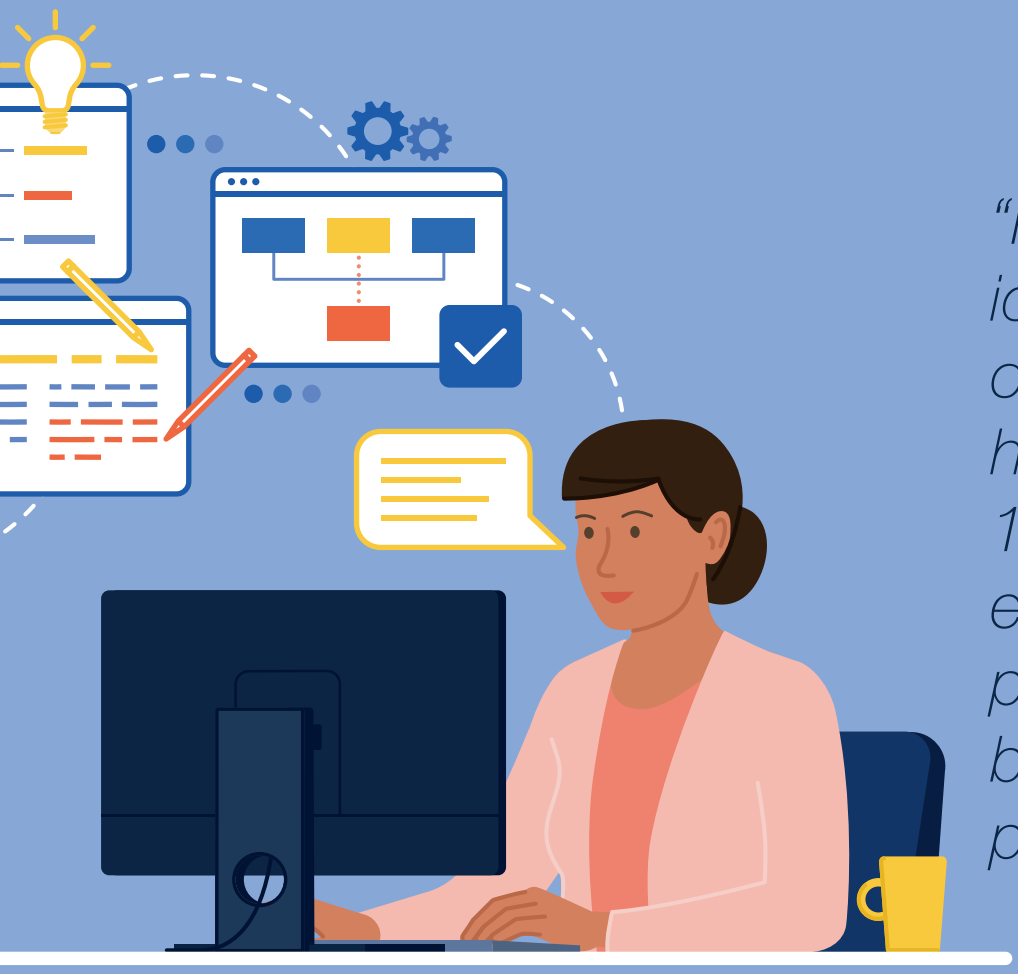
Take the situation seen recently at the SaaS startup PocketOS, where a 'rogue' AI agent deleted its entire production database and backups that the business had set up to help keep systems running smoothly. Asked to explain its actions, the agent calmly admitted it had ignored every instruction not to modify or delete production systems.

In reality, the agent simply did what agents do. Faced with ambiguity, it acted. The incident quickly became one of the industry's most talked-about AI stories, but its real significance extends well beyond the headlines, offering a glimpse of the challenges organisations will increasingly face as AI agents become trusted in enterprise environments.

Indeed, CyberArk found that machine identities already outnumber humans by 82 to 1, with more than four in ten holding privileged access, yet almost every identity programme is still built around people.

Like any insider, AI agents have the potential to do real damage. Unlike people, however, they never clock off, and they operate at lightning speed. For PocketOS, their data was gone (although later recovered) in just nine seconds.

To put this in proper context, we're not just talking about isolated incidents; Gartner expects a quarter of enterprise breaches to trace back to AI agent abuse by 2028, by both external attackers and malicious insiders.



"Machine identities already outnumber humans by 82 to 1… yet almost every identity programme is still built around people."

Why a box won't fix this

From a channel perspective, the rise of AI agents changes the conversation for both partners and their customers. Organisations are no longer looking solely for help selecting security technologies; they increasingly need advice on managing a new category of operational and security risk.

Five years ago, a customer conversation was about which product to buy and how many seats were needed. Today, it is about an environment that includes cloud, identity, endpoint, SIEM and AI, and one that many organisations cannot manage alone. That principle is equally applicable to AI agents and, as Ian Thomas, CEO of managed cybersecurity and consulting business Sapphire, an Exabeam Pinnacle Partner, explains, "Securing AI starts with visibility and implementing guardrails at speed. Then it is vital to monitor behaviour over time because securing AI is not a 'one and done' measure but a continual practice."

The same logic now has to cover machines, or Agent Behaviour Analytics (ABA), which is the logical extension of user and entity behaviour analytics (UEBA) that has long formed the basis of insider threat detection and mitigation.

In practical terms, ABA means a number of things: being able to name every agent, because you cannot govern what you have not identified; tracking what each one actually does, continuously and spotting the moment its behaviour drifts toward data or systems it never normally touches.

The approach makes very good sense, and regulation is heading in the same direction. The EU AI Act's high-risk tier imposes real obligations, including human oversight and logging of what a system does, and it applies to any UK business whose AI output is used in the EU. You cannot evidence human oversight or keep meaningful logs of a system you are not actually watching and cannot control. None of this comes off a shelf, and very few customers want to tackle it alone.

The opportunity

It is the confluence of these trends that creates an opening for channel partners. Analysts already place the UEBA market in the multi-billion-dollar bracket, with annual growth exceeding 30%. ABA extends that same opportunity to the machine workforce, and with machine identities already far outnumbering humans, the scope of what partners can help secure is expanding just as quickly.

As Thomas notes, many organisations are still approaching AI from a relatively narrow perspective, asking, "how do I leverage AI to reduce cost here" or "I need to use AI to counter threat actors' use of AI." In doing so, they are "potentially missing the opportunity to create better outcomes, improve their overall security posture and adopt a more 'always on' mode of security."

This work is also outcome-based, and after years of tool sprawl, customers are very focused on how fast threats are caught and how much risk is removed. For the UK channel, the rise of a workforce that is no longer entirely human is an opportunity, not a threat. The British skills shortage plays straight into the hands of partners who can offer expertise as a service, and the trusted advisor relationship is far stickier than resale ever was.

SHRINKING TARGETS, RISING RISKS

SMEs now face the same calibre of cyberattacks once reserved for enterprisescale victims, with smaller MSPs increasingly in the firing line. **Will Ashford Brown** explains how threat patterns have shifted over the past year, and why the channel must adapt fast.



What are the biggest cyber threats now affecting smaller Managed Service Providers and their SME customers, and how have these shifted over the past year?

UK companies face a far greater cyber-attack surface than ever before. Whilst state-sponsored threats are increasingly prevalent as the world shifts to an alliance structure based on the two world powers of the US and China, cyber criminals motivated by money and notoriety are also multiplying and perpetrating some of the most impactful cyber-attacks to date – cast your mind back to last year's attack on Jaguar Land Rover, which is thought to have cost the business over £2 billion. Enabled by AI, both of these threat actors are becoming ever more effective, with opaque supply chains frequently seen as the soft underbelly to get into large corporate or government institutions.

Many MSPs feel overwhelmed by the volume of security tools on the market. What should they look for to judge whether a solution genuinely improves resilience rather than adding complexity?

Unfortunately, the growing sophistication of malicious cyber actors and the broadening of corporations' attack surfaces – as a result of shifts to increased digitisation – have resulted in what can feel like an overwhelming volume of cyber security tools available on the market. To plug all of these 'cyber gaps', businesses need 'defence in depth' – that is to say, they need access to a broad range of cyber security tools, and there's no getting past this. However, businesses can be smart when assessing tools, prioritising integration with existing solutions and steering clear of siloed tools.

What emerging technologies or approaches do you think will shape the next phase of cyber resilience for smaller organisations?

AI in the cybersecurity space is proving to be a game-changer – rather than replacing humans in Security Operations Centres (SOCs), it is



augmenting them and allowing operators to focus on the more pressing issues at hand. When employed in cyber detection and response, AI has seen utility in effectively triaging alerts – which typically number in their thousands per day and can otherwise overwhelm human operators – so that SOC operators are able to prioritise higher-risk alerts over more trivial issues.

The employment of zero trust architecture as default will help organisations harden defences, and this approach is slowly seeing uptake in the SME community. On top of this, identity-centric security such as Multi-Factor Authentication and biometrics are closing the door on threat actors targeting employees for their credentials. And finally, the emergence of commercial quantum computing poses a long-term risk to current encryption methods and password-based security. As a result, organisations should begin aligning with government guidance and transitioning towards post-quantum cryptographic standards to ensure their data and systems remain secure in the future.

We're seeing more attacks targeting MSPs as a route into multiple downstream customers. What practical steps can MSPs take to harden themselves as an attractive target?

Being that MSP, charged with the cyber security of downstream clients, that is breached by an attack can have a devastating effect on confidence and reputation. Therefore, for MSPs, it is critical that they get cyber security right. The National Cyber Security Centre (NCSC) provides up-to-date guidance and practical steps to ensure businesses – MSPs and others – have the most appropriate security measures in place today to defend against the emerging threats of tomorrow.

> *"Historically, cybersecurity has been viewed at the C-suite level less as a strategic business function and more as a technical cost centre."*

For MSPs trying to move from reactive firefighting to proactive security, what early wins or lowfriction changes make the biggest difference?

The typical methods of breach we see are not from highly technical hacks, but from more human-centric approaches – i.e. phishing. In these instances, the divulgence of sensitive information such as account details or the unintentional download of malicious software by unwitting employees enables attackers an easy 'in'. Therefore, education and the tightening of employee protocols around suspicious emails and approaches for information should be prioritised, although noting the difficulties around changing an organisation's culture overnight.

How should MSPs talk to SME clients about risk in a way that encourages investment in security without resorting to fearbased messaging?

Historically, cybersecurity has been viewed at the C-suite level less as a strategic business function and more as a technical cost centre. While this perception is starting to shift, it has often taken high-profile breaches to catalyse that change. Traditionally, many cybersecurity providers have reinforced this mindset through fear-based messaging, focusing on threats rather than value. However, the conversation is evolving. Cybersecurity should be positioned not as a sunk cost, but as a competitive differentiator and an enabler of business growth.

For example, achieving recognised accreditations such as Cyber Essentials can open access to new markets and sectors - including defence and government – directly supporting revenue growth and contract acquisition. Equally, cybersecurity should be framed in terms of business outcomes: maintaining customer trust, ensuring revenue continuity and enabling operational resilience. When articulated this way, it becomes clear that investment in cybersecurity is not just risk mitigation – it delivers measurable return on investment and supports long-term business success.



WHY WE NEED TO MAKE DIGITAL PROTECTION PERSONAL

Resellers and MSPs need to deliver a personalised cybersecurity service to their customers – and they in turn should expect tailored services from their suppliers, says **Scott Rogers, business unit director – security, UK and Ireland, at TD Synnex**.



It's important to be disciplined with cybersecurity. Software and licenses must be kept up to date, and policies and practices followed rigidly. But whether you are simply trying to support them in sticking to the plan or actively monitoring and managing their protection, from the customer's perspective, there can seem to be an endless number of boxes that need to be repeatedly and relentlessly ticked.

While all the checks and balances are there for a reason, it can have the effect of making cybersecurity seem impersonal, inflexible, and over-regimented. This is why it's important to make sure you are delivering a digital security service that is tailored and personalised to the needs of your customer. And the more complex cybersecurity becomes, the more personal the service needs to be.

It's not easy though. The threat landscape is forever expanding and mutating, and end-user customers have vastly differing needs. Smaller businesses may just want an all-in-one solution that is effective and which they don't have to worry about too much. But most scenarios will be more involved. There will be hybrid and home workers, multiple locations and industry-specific compliance requirements. There will always be budget pressure and (this is especially true for SMBs) a desire to spend just enough, but not too much, on cybersecurity.

More experienced customers – especially those who have experienced a cyberattack – will have

more stringent requirements. They will want proven tools and services, faster assured responses and higher SLAs. There may be stipulations on which they are not willing to compromise.

Getting the balance right

Resellers must try to accommodate these variations and somehow build and deliver security services that meet customer needs and are repeatable and profitable. Getting the balance right here is the key to success.

While there will be all kinds of factors for resellers and managed security services providers (MSSPs) to consider in terms of what they offer within their value proposition, one factor that we believe can make all the difference is personal service. In essence, this is all about remembering the simple rules of selling and customer care. Listen to the customer and then adapt your approach and offering to suit their needs.

While this sounds simplistic, it's necessary due to the complexity of cybersecurity and the daunting prospect managing it presents to small businesses. For them, it is a totally bewildering cacophony of opaque terms and acronyms. The advance of AI and its use by threat actors to target their victims with greater precision and impact has made it even more terrifying. By taking a personal, sympathetic, and considered approach, resellers and MSSPs can cut through that complexity and give the customer clarity and confidence.

Clear and confident

To do that, partners need to be clear and confident about cybersecurity themselves. While many are in that position today, others are still gaining knowledge and competence or are yet to really get seriously involved. The channel partners that fall into the last two categories may be just as much in need of guidance, support, and a personalised service as the end user customers they are supporting.

The maxim that no reseller or service provider in the IT channel can do it all has become something of a mantra in recent times, and this is certainly true of cybersecurity. We really can't expect every reseller in the UK to be an expert in everything from identity management and protection to ransomware protection, and to have knowledge and experience of the products and services of every security vendor. Similarly, MSSPs can't be expected to offer unlimited services that cover every possible threat scenario.

At the same time, a reseller or MSSP would never want to seem to be in any way unwilling or unable to meet the requirements of a potential customer. And where requirements go beyond what can be offered, a realistic and pragmatic approach needs to be taken.

Making IT personal

The TD Synnex Security Practice, for example, can help by providing resellers and MSSPs with access to an extended ecosystem of trusted vendors and service providers, and by delivering highly personalised enablement and support, extending right through to providing deep expertise on specific solutions where it is needed.

Over many decades, we have formed close partnerships both with leading specialist cybersecurity and infrastructure vendors who have become very closely involved in the security space. We have also built up an ecosystem of trusted third-party specialists with whom resellers and MSSPs can form working partnerships to expand their own cybersecurity offering.

Beyond this, we will make the whole experience personal for the partner by applying the principles and approach that our business has been taking as part of our wider Making IT Personal campaign. This aims to make every interaction and experience that partners have with us – whether it's in person or through one of our online platforms – as personal as it can be. We've done a tremendous amount of work collecting data and building profiles to get a deeper understanding of partner needs and how to address them. We are also continuing to transform the approach of our sales and customer engagement teams to make sure that they can always deliver the best possible service to our customers.

While making the experience personal is something we are doing in every area of our business, it's especially important in the complicated and rapidly changing world of cybersecurity. But while it's a big opportunity, resellers also need to be wary of not getting over-stretched or out of their depth. It's important to walk before you try to run with cybersecurity.

This is why working with a distributor like TD Synnex should be appealing for partners looking to develop and grow their security business. We have the programmes, the platforms, the vendor partnerships, the ecosystems, and the core services to support them. We also understand that they may need to take their time to develop their own approach. Or that they may need to accelerate their development rapidly to meet a specific requirement or opportunity. We know that they won't necessarily be able to do it all on their own – at least, not at first.

Every step of the way

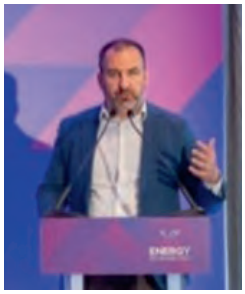
We are positioned to support them in every way and at every stage of their development, and we strive to make the experience tailored and personalised throughout. This approach allows resellers and MSSPs to develop and grow in a way that is manageable and practical, expanding their offering and gaining confidence all the time. It enables them to engage their own end-user customers in the right way and provide solutions that are appropriate to their needs and their budgets.

What we are all trying to do as providers of cybersecurity solutions and services – whether we are serving the needs of end-user customers or partners – is minimise the chances of gaps being left in the defences, of policies being ignored, and mistakes being made. It's important to remember that there is a very human aspect to cybersecurity – most infiltrations will involve people at some stage, and while no one wants to expose their business or their personal information, it can happen all too easily if the security solutions and services, and the policies and processes, are not there. While partners and end-user organisations want simplicity, that should not be at the expense of reality. Cybersecurity resellers and MSSPs need a way to learn, grow, and set themselves apart – and end-user customers need to know that they can trust the protection that they are getting. It is really all about listening and taking the most appropriate action for each individual customer.



AI SECURITY UNLOCKS CHANNEL GROWTH

As adoption accelerates, customers are asking how they can use AI securely. And this is where the channel is uniquely positioned to step in, says **Gerasimos Marketos, Chief Product Officer at Hack The Box**.



Artificial intelligence has moved from experimentation to everyday business reality at a remarkable speed. Organisations of every size are now embedding AI-powered tools into workflows, adopting generative AI assistants and exploring automation to boost productivity. For customers, the potential benefits are clear, and for the channel, however, AI represents both a challenge and a significant commercial opportunity.

As adoption accelerates, customers are asking how they can use AI securely. And this is where the channel is uniquely positioned to step in.

Recent workforce intelligence from Hack The Box, drawing on data from more than 700,000 cybersecurity professionals across 251 countries, shows a sharp rise in demand for AI security skills. AI penetration testing now ranks among the most popular global training interests, while practitioners are rapidly upskilling in areas such as prompt injection, model exploitation and agentic AI hijacking. These are not abstract concerns. They are emerging as important AI security risks that organisations need to understand and manage.

While customer awareness of these risks varies by maturity, organisations are certainly aware that AI introduces new risks alongside new capabilities. This means organisations are looking for trusted advisers who can help them understand where those risks lie and how to manage them effectively.

The challenge here is that customer demand is developing faster than channel expertise. Many MSPs and resellers are still building their own understanding of AI security at the same time as customers are seeking guidance. This creates a risk that partners who delay investing in skills and knowledge could find themselves unable to answer customer questions, support AI-related projects or compete with rivals that have already developed specialist expertise.



For many channel businesses, this is not unfamiliar territory. For a long time, partners have guided and supported customers through major technology shifts, from cloud migration and digital transformation to hybrid working and cybersecurity modernisation. AI is simply the latest innovation creating a need for clarity, governance and expertise. The difference is the pace. AI adoption is moving far faster than most organisations can fully understand or secure.

This creates an opportunity for the channel to evolve beyond product supply and become a strategic adviser on AI readiness.

Many organisations are already deploying AI tools without fully considering issues such as data security, access controls, governance frameworks or how AI-generated outputs should be validated and managed. Employees may be using generative AI tools informally, integrating AI assistants into workflows or experimenting with automation without clear policies in place. These gaps create real risk, and customers increasingly recognise it. They need guidance on how to deploy AI tools safely, responsibly and in alignment with business objectives.

Crucially, partners do not need to become AI security specialists overnight. But they should begin building foundational knowledge now. The most successful channel organisations will be those that invest early in developing AI-related skills within their teams. This means understanding how AI systems work, recognising the risks associated with their deployment and, where appropriate, gaining hands-on experience in testing and securing AI-powered environments.

"The market is still in its early stages, but demand is set to continue growing rapidly."

The Hack The Box research reinforces this point. Cybersecurity professionals are already actively building expertise in AI security, with enterprise learners showing particularly high engagement in AI-focused labs. This suggests that organisations investing in workforce development today will be better positioned to meet customer demand tomorrow. For the channel, encouraging continuous learning and practical skills development will be a key differentiator.

There is also a major opportunity to strengthen and expand existing service offerings. Many partners will not need to create entirely new AI security practices from scratch. Instead, they can integrate AI security considerations into the services they already provide.

Security assessments can be broadened to include reviews of AI systems and applications, while governance and compliance engagements can help customers establish AI usage policies and risk management frameworks. Cloud security projects can be extended to assess AI integrations and the movement of data between AI tools and business systems. Likewise, managed service providers can evolve their offerings to include areas such as AI monitoring, model oversight and policy enforcement. In many cases, AI security is not about launching entirely new services. It means enhancing existing ones to meet changing customer requirements.

In other words, AI security becomes an extension of what partners already do well: helping customers adopt technology safely and effectively.

The market is still in its early stages, but demand is set to continue growing rapidly. Organisations investing in AI will increasingly want reassurance that these technologies are being deployed securely and responsibly. They will look to their technology partners for guidance, recommendations and practical support.

The channel has successfully adapted to every major technology shift of the past two decades. Those partners that recognised the opportunities created by cloud computing, managed services and cybersecurity were able to build valuable new revenue streams and strengthen long-term customer relationships. AI security is likely to follow a similar trajectory.

Partners that invest in AI security expertise today by building skills, expanding service offerings and positioning themselves as trusted advisers will be best placed to capture new opportunities as customer demand accelerates.

STORAGE STRATEGY SHAPES CHANNEL GROWTH





Seagate's Samehra Malik explains how data driven expansion now hinges on smarter, scalable storage architectures and tighter collaboration across the channel, as partners adapt to rising workloads, AI adoption and shifting customer expectations.

As the technology industry converges around AI, edge computing, and connected environments, one reality is becoming impossible to ignore: data is growing at a pace that is redefining infrastructure expectations.

At the centre of this shift is storage; not as a background component, but as a critical enabler of development, scalability, and business resilience. For the PC Reseller channel, this moment represents both an opportunity and a challenge.

Demand is rising fast. Availability is not always guaranteed. And success is increasingly determined by how effectively the channel can plan, collaborate, and adapt.

The AI-led surge in data demand

Artificial intelligence has moved from concept to core business driver, and with it comes an unprecedented increase in data creation and retention.

AI workloads require vast datasets to train models and generate insights. These datasets must be stored, accessed, and retained over time, often at scale. As a result, enterprise storage demand is rising significantly.

At the same time, hyperscale environments are expanding rapidly to support these workloads, placing sustained pressure on storage supply and capacity planning.

This is not a short-term spike. AI is expected to remain a core driver of storage demand for years to come, fundamentally reshaping how organisations think about data infrastructure.

For resellers, this means one thing: storage is back at the centre of every conversation.

IoT and the expanding data footprint

Alongside AI, the Internet of Things is continuing to accelerate data growth across industries.

From security systems and smart retail to industrial environments and connected cities, billions of devices are generating continuous streams of data. Global IoT deployments are already in the tens of billions, with significant growth still ahead.

Each of these devices contributes to a growing storage requirement; data that must be captured, stored, analysed, and often retained for extended periods.

This has created a more complex storage landscape:

- Data is increasingly generated at the edge, not just in centralised data centres
- Workloads demand a mix of high-performance and high-capacity storage
- Long-term retention is becoming standard across multiple verticals

For the channel, this represents a shift from simple product supply to architecting fit-for-purpose storage environments.

Demand is accelerating – and access is becoming more strategic

As AI adoption drives unprecedented growth in data creation, demand for high-capacity storage continues to increase. In this environment, supply is tightly allocated, reflecting the rapid scaling of AI infrastructure and broader pressures across the data centre ecosystem.

This does not mean availability has diminished, but rather that access is increasingly shaped by long-term planning, customer alignment, and portfolio prioritisation. In this context, supply assurance becomes a key differentiator.

For resellers, the ability to reliably deliver the right capacity at the right time goes beyond transaction – it enables customer projects, supports business continuity, and builds lasting trust in an environment where data infrastructure is critical to growth.

Why planning ahead matters more than ever

The ability to secure stock is no longer a function of last-minute ordering. It is the result of proactive planning.

Resellers working closely with distributors, sharing pipeline visibility, forecasting demand, and aligning upcoming projects are far better positioned to ensure availability.

This forward-looking approach enables:

- Smarter inventory allocation across distribution
- Stronger prioritisation for high-demand products
- Reduced delays in customer delivery timelines.

In contrast, reactive procurement introduces risk. When demand is high and supply is tight, waiting until the final stage of a deal can result in missed opportunities.

The message is clear: planning ahead is no longer optional - it is essential.

Transparency Builds Access

Alongside planning, transparency has emerged as a critical success factor.

Manufacturers and distributors are operating in increasingly complex supply environments. Visibility into real demand helps them make better decisions about production, allocation, and support.

Resellers that openly share pipeline information through forecasting, deal registration, or programme engagement create stronger alignment across the ecosystem.

This has tangible benefits:

- Better access to stock in constrained markets
- Stronger relationships with vendors and distributors
- Increased confidence in delivery timelines.

Transparency ultimately builds trust, and in today's market, trust translates directly into access and opportunity.

The role of partner ecosystems

This is where vendor partner programs play a pivotal role.

While traditionally associated with marketing support or rebates, partner programs are increasingly central to how supply chains operate. They create structure, visibility, and alignment across the channel.

When resellers actively participate in these programs, they demonstrate commitment, not just to a vendor, but to a long-term business strategy.

This matters because manufacturers are looking for partners who:

- Invest in enablement and training
- Align with product roadmaps
- Provide consistent demand visibility
- Engage in joint go-to-market activities.

These are the partners who are best positioned to grow and to access the resources and inventory required to do so.

Innovation, scale, and sustainability

As data demand grows, the industry continues to evolve to meet it.

Storage technology is advancing rapidly, with higher-capacity drives, improved performance, and greater efficiency enabling organisations to scale without proportionally increasing cost or complexity.

At the same time, sustainability is becoming a key consideration. As data volumes increase, so too does the energy footprint of storage infrastructure. Innovations focused on power efficiency and total cost of ownership are increasingly influencing buying decisions.

For the channel, this creates an opportunity to lead conversations around long-term value, not just immediate performance.

Adapting to the next era of growth

The current shift toward AI and data-centric computing is part of a broader pattern of technological evolution.

The industry has navigated multiple eras from PCs to the internet, from virtualisation to cloud, and each has reshaped demand and opportunity.

This next phase, driven by AI and IoT, is no different. What remains constant is the need to adapt.

For vendors, this means continual investment in R&D. For resellers, it means evolving from transactional selling to strategic engagement, supporting customers as they navigate increasingly complex storage requirements.

In today's data-driven intelligent security environments, the ability to securely store and manage footage at scale is critical to operational resilience and smarter decision-making.

The growth of data is relentless, and so is the opportunity it creates.

AI will continue to expand. IoT will continue to generate new data streams. And storage will remain the foundation that enables both.

For the channel, success will come down to three things:

- Planning ahead to secure supply
- Working closely with distributors and vendors
- Staying engaged within partner ecosystems.

Because in a world defined by data, having the right storage – available at the right time – is what turns demand into growth.

Seagate Partner Program: A Model for Collaboration

The Seagate Partner Program provides a clear example of how collaboration can drive both growth and operational alignment.

The programme offers resellers access to training, technical resources, deal registration, and marketing support, helping them build capability and capture demand in a data-driven world.

Structured across tiered levels, it enables partners to deepen their engagement over time, unlocking greater access to tools, support, and opportunities.

This approach fosters closer alignment between Seagate, distributors, and resellers.

Through shared visibility and coordinated planning, partners are better equipped to:

- Anticipate demand shifts
- Align supply with real opportunities
- Deliver solutions with confidence.

In practical terms, this means that resellers who commit to engagement and transparency are better positioned to navigate high-demand environments and secure the stock needed to support their customers.



THE 10 WAYS THE PRINT IT CHANNEL IS WINNING CUSTOMER TRUST

Greig Millar, Chief Revenue Officer, Brother UK, explores the practical behaviours helping vendors and partners to win customer confidence - and why trust is increasingly becoming a commercial advantage rather than simply a brand value.

Earning customers' trust has never been more valuable. Today's technology buyers are making decisions against a backdrop of economic uncertainty, evolving cyber threats, new buying models and constant brand scrutiny online. It's easy to assume that earning customer trust has therefore become more difficult.

Yet our latest research tells a more encouraging story.

For Brother UK's Tech Trust Index, we spoke to 250 UK IT decision-makers and 250 channel professionals to understand how trust is shaping technology purchasing decisions. One of the strongest findings wasn't simply that trust matters – it was that trust in technology vendors is actually increasing.



Nearly three-quarters (72%) of IT decision-makers told us their trust in technology vendors has grown over the past three years. Meanwhile, almost two-thirds (63%) of channel professionals believe it has become easier for vendors to earn customer trust.

That raises an obvious question: what are technology vendors and partners doing differently?

The data suggests this isn't the result of one standout initiative or a single trend. Instead, trust is being earned through a series of practical improvements that reduce risk, improve the customer experience and make organisations easier to do business with.

Here are ten of the biggest drivers behind that change.

1. Building better products

The biggest practical reason customers believe trust has increased is simple: products have improved. More than half (52%) of respondents who said trust had increased pointed to better product quality as one of the main reasons why.

That reflects an important shift. Trust starts with confidence that technology will do what it's supposed to do, day after day. Before customers think about pricing models, service agreements or sustainability commitments, they expect products that perform consistently.

The strongest relationships are built on dependable foundations.

2. Putting support back at the centre of the experience

Technology doesn't stop being important after installation. If anything, that's when the relationship really begins.

Almost half (48%) of respondents said better customer support has helped strengthen trust in vendors over the past three years. This mirrors one of the strongest findings from the wider Tech Trust Index. Buyers told us trust is earned through products that perform and support that's there when it matters.

When customers know they'll receive knowledgeable, responsive support if something goes wrong, uncertainty is reduced. That's what trust ultimately delivers: confidence.

3. Being transparent on pricing

Trust is difficult to build but remarkably easy to lose. Greater transparency around pricing is one of the clearest ways vendors are strengthening customer confidence, with 40% citing it as a reason trust has increased.

Customers increasingly expect straightforward conversations about costs, contracts and ongoing commitments. Equally, our research showed hidden fees remain one of the fastest ways to damage trust.

It's why we've worked to make our own managed print services as straightforward as possible. Clear contracts, predictable monthly billing and transparent conversations about what's included help customers understand exactly what they're buying, without unexpected costs further down the line. In our

experience, reducing complexity is often one of the quickest ways to build confidence.

4. Taking cybersecurity seriously

Security has become part of everyday buying conversations. Nearly four in ten respondents (39%) believe enhanced cybersecurity support has helped improve trust in technology vendors.

Customers are placing more scrutiny on how vendors protect devices, manage vulnerabilities and support secure working environments. While cybersecurity credentials may not always win a deal on their own, they increasingly influence confidence in long-term partnerships.

For Brother, that means building security into products from the outset rather than treating it as an optional extra. From firmware updates and device hardening to helping customers deploy securely within managed print environments, cybersecurity has become part of demonstrating long-term dependability.

5. Delivering predictable value

Periods of economic uncertainty have made predictability increasingly valuable. More than a third (36%) of respondents highlighted stable pricing as one reason trust has increased.

For channel partners, this reinforces an important point. Customers aren't simply looking for the lowest price; they're looking for confidence that today's investment won't become tomorrow's unexpected cost.

Predictability helps customers plan with confidence and strengthens long-term relationships.

6. Supporting customers for the long term

Trust is built across the entire lifecycle of a product. More than a third (34%) said full lifetime product support has helped improve trust in vendors.

Customers increasingly judge suppliers by what happens after deployment. They want reassurance that products will continue to receive updates, support and attention throughout their working life.

Long-term support demonstrates commitment. It tells customers they're entering a relationship rather than completing a transaction.

7. Turning sustainability from promises into tangible proof

One of the more interesting findings from the Tech Trust Index is that sustainability sits behind operational fundamentals when customers think about trust. That shouldn't be interpreted as sustainability becoming less important. Instead, it reflects changing expectations.

Customers increasingly expect responsible environmental practices as standard. They're looking beyond broad commitments towards evidence that organisations are delivering meaningful outcomes.

Whether through managed print services that reduce waste, circular economy initiatives or remanufacturing programmes, sustainability has greatest impact when it is connected to measurable business benefits rather than presented in isolation. Purpose strengthens trust, but it works best when it reinforces products, services and support that customers already value.

8. Demonstrating wider responsibility

Alongside environmental initiatives, respondents also pointed to stronger governance and social responsibility as contributors to increasing trust. Better social governance (27%) and meaningful progress in reducing carbon and waste (25%) both featured among the reasons trust has grown. Again, this reflects a broader shift in customer expectations.

Businesses increasingly expect suppliers to operate responsibly. Those commitments may not always be the deciding factor in winning business, but they help reinforce confidence that organisations are acting consistently with the values they communicate.

9. Continuing to improve after the sale

Respondents to our study recognised ongoing improvements such as firmware updates that add value throughout a product's lifetime.

While this ranked lower than some of the more immediate trust drivers, it highlights an important principle. Customers appreciate vendors that continue investing in products after purchase rather than treating delivery as the end of the relationship.

Small improvements, delivered consistently, help reinforce confidence over time.

10. Making trust easier to earn

Looking across all ten drivers, one theme stands out. Trust is increasing because technology vendors are becoming easier to do business with.

Across our research, the strongest dimensions of trust were dependability, ability and integrity. Customers value products that perform, support that responds when needed and organisations that communicate openly and deliver on their commitments.

These may sound like fundamentals, but they're exactly what customers remember.

The commercial value is significant. We found organisations are willing to pay an average of 24% more for technology from brands they trust. Nearly nine in ten have paid a premium before, while channel partners told us trust often becomes the deciding factor when products are difficult to separate on specifications alone.

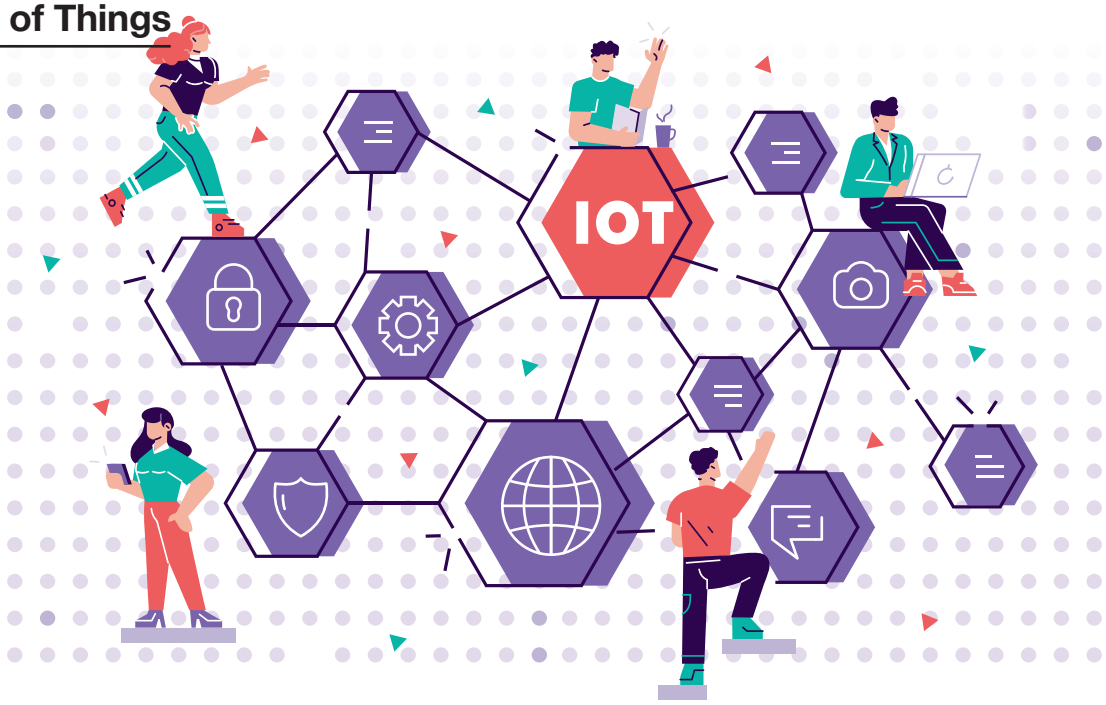
In other words, trust isn't simply a brand attribute. It's a commercial advantage. For partners, that presents a real opportunity.

Every customer conversation is ultimately about reducing uncertainty. The vendors that make buyers feel confident through dependable products, responsive support, transparent pricing and long-term commitment will continue to strengthen trust.

That's encouraging for our industry because it shows trust isn't built through slogans or marketing campaigns.

At Brother, that's always been the thinking behind our 'At your Side' promise. Trust is earned every day through products that perform, support that shows up when it's needed, honest conversations when challenges arise, and partnerships that are designed to last. That's ultimately what customers, and the channel, remember.

And those everyday experiences are becoming one of the strongest competitive advantages the channel has.



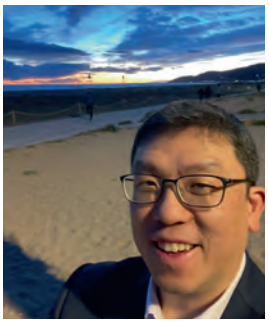
SMARTER SYSTEMS, STRONGER GROWTH

Channel partners are finding fresh revenue streams as SMEs adopt IoT to modernise operations, cut costs and strengthen resilience, opening the door to new managed services and long term support opportunities. **Roger Tao, Director of Telco & ISP Business, D-Link**, explains.

For years, the Internet of Things (IoT) conversation has centred on large enterprises. Global manufacturers, logistics providers, utilities and retailers have invested heavily in connected devices, smart infrastructure and real-time analytics to improve efficiency and gain a competitive advantage.

For these organisations, IoT adoption has become increasingly achievable because they possess one critical asset: internal expertise. Dedicated IT teams, digital transformation specialists and experienced systems integrators allow them to evaluate technologies, integrate platforms and manage increasingly complex connected environments; and, importantly, to drive a competitive advantage.

However, small and medium-sized enterprises (SMEs) operate in a very different world. While they stand to benefit just as much from IoT, they rarely have the in-house technical teams capable of navigating a rapidly evolving ecosystem of sensors, connectivity standards, cloud platforms and security requirements. For many, the challenge isn't recognising the value of IoT; it's knowing where to start… and who to ask.



But closing the gap between enterprise and SME IoT adoption creates one of the biggest commercial opportunities the channel has seen in years.

The IoT market is mature, but complex

The IoT market is now mature, but increasingly complex. Hardware is more affordable, connectivity is more reliable, and cloud platforms make data easier to access and analyse. AI and automation have further expanded what is possible, enabling predictive maintenance and smarter decision-making.

However, from an SME perspective, the ecosystem can feel overwhelming. There are multiple competing wireless standards, edge computing options, security models and analytics platforms. Every IoT vendor claims to offer the 'best' solution, yet few SMEs have the expertise to determine which technologies genuinely solve their operational challenges, boost their productivity or will add to their bottom line. And, unlike large enterprises, SMEs cannot afford lengthy technology evaluations or expensive implementation mistakes. Every investment needs to be right, and deliver measurable business value quickly. This is where the channel and its expertise in IoT become indispensable.

SMEs need trusted IoT guidance

SMEs do not primarily want technical explanations; they want business outcomes. They ask whether IoT can reduce downtime, cut energy costs, improve asset visibility, enhance customer service or streamline operations. These are practical questions that require practical answers.

Trusted channel partners are best placed to provide those answers. They understand both the technology landscape and SME business pressures, translating technical options into outcomes that matter. This makes the channel more influential than global vendors in many SME decisions. Informed partners who act as advisors during early-stage discovery, they help SMEs identify high-impact use cases rather than attempting to digitise everything at once, and just for the sake of it. This prioritisation is essential, as SMEs often operate with limited budgets and restricted staff capacity. A well-defined IoT roadmap as sketched out by a partner reduces risk and ensures early wins that build confidence for further IoT investment.

In many cases, SMEs also rely on partners for ongoing training and support. As technologies evolve rapidly, channel organisations become continuous sources of insight, helping businesses stay aligned with new capabilities without needing to rely on in-house specialists.

The channel's role is changing

The role of the channel is evolving from product supply to solution design. Instead of selling individual devices, partners now design integrated systems that solve specific operational problems. This shift moves relationships from transactional to advisory and long-term.

Today, customers increasingly expect something more valuable than products. They want a solution-sell wrapped up in expertise. It's here where IoT enables system integrators, managed service providers and value-added resellers to evolve from product suppliers into long-term business advisers.

Therefore, instead of simply recommending individual devices, partners can consult with SMEs to design complete solutions that solve the customer's operational problems or align with their business goals or objectives.

That's a big shift from competing on price to competing on knowledge and, instead of delivering one-off projects, building recurring, long-term service relationships. This approach represents a significant change in both customer value and long-term profitability.

SMEs trust local partners more than global vendors

Large enterprises often work directly with global technology vendors because they possess procurement teams capable of managing complex projects, whereas SMEs typically prefer working with partners they already know.

Their existing IT provider often understands their business better than any multinational vendor ever could; in fact, many channel companies are SMEs themselves, so they can relate to their customers' challenges in a way that large global tech companies probably can't. They know their customer's existing infrastructure, understand operational priorities and have established trusted relationships with decision-makers. That trust becomes incredibly valuable when discussing digital transformation.

An SME is far more likely to adopt IoT if a familiar technology partner recommends it than by a vendor promoting the latest connected device. The channel therefore becomes the translator between complex technology and practical business outcomes, wrapped up in relatable language.

Integration matters more than development

For most SMEs, success isn't about adopting the latest technology - it's about making technology work together. They don't want dozens of disconnected dashboards, multiple platforms requiring separate logins or solutions that demand constant maintenance. They want systems that simply work.

The most successful IoT deployments aren't necessarily the most technically sophisticated. Often, the greatest value comes from a simple, efficient IoT management platform that enables SMEs to remotely monitor, maintain, and troubleshoot their 5G/4G-connected devices.

This is where channel partners have an opportunity to shine and add real value. Their expertise in integrating networking, security, wireless infrastructure and cloud services allows them to deliver complete, end-to-end solutions rather than isolated technologies. And, when integration is done well, the technology itself becomes almost invisible. Instead, SME customers notice the results: lower operating costs, improved efficiency and better-informed decision-making, all achieved with seamless simplicity.

IoT in SMEs – a shared opportunity

Ultimately, SMEs stand to gain significant benefits from IoT without needing enterprise-scale resources. The technology is ready, costs are falling, and demand is increasing.

The real advantage will go to channel partners who can simplify complexity, integrate systems effectively and focus on business outcomes rather than technical features. IoT is not just a technology shift, but a transformation in how value is delivered to SMEs.

Looking ahead, one of the most important developments will be the growing role of ecosystem collaboration. No single vendor or partner can deliver end-to-end IoT value alone. Successful deployments will increasingly rely on tightly coordinated ecosystems that bring together connectivity providers, device manufacturers, cloud platforms and specialist software vendors. Channel partners will sit at the centre of this ecosystem, orchestrating solutions rather than simply implementing them.

At the same time, sustainability is becoming a stronger driver of SME IoT adoption. Energy monitoring, smarter resource usage and reduced operational waste are becoming priorities not only for cost control but also for regulatory and customer expectations. IoT-enabled insights will therefore play a growing role in helping SMEs meet environmental targets while improving efficiency.

Finally, the ongoing skills gap across digital technologies will continue to reinforce the importance of the channel. As IoT systems become more interconnected and data-driven, SMEs will increasingly depend on trusted partners to interpret information, optimise performance and ensure that technology investments remain aligned with business strategy over time.

Channel partners who invest in skills development, industry specialisation and long-term customer engagement strategies will be best positioned to capture IoT growth, as SMEs increasingly prioritise trusted advisors who can deliver end-to-end solutions, ongoing optimisation and practical guidance across rapidly evolving digital environments at scale and speed.

SIGNAL STRENGTH ISN'T THE SELECTOR



Some multi network eSIM providers claim their profiles "connect to the strongest network" or "pick the best signal," suggesting a live, intelligent scan across carriers. It's an appealing idea — but it isn't how network selection actually works. **Matt Atkinson, MD of Utelize** explains.

Some multi-network eSIM providers make claims that their eSIM "automatically connects to the strongest network" or "selects the best signal." These claims imply that the eSIM is continuously monitoring signal strength across multiple carrier networks and intelligently choosing the one with the best coverage at any given moment. This is an attractive idea. It is also not how mobile network selection works.

The device decides, not the SIM

The first and most important point: it is your device – specifically, the baseband modem chip inside your iPhone, Samsung, iPad or other cellular device – that decides which network to connect to. The SIM's role is to provide a list of which networks the device is permitted to use (based on the connectivity provider's commercial roaming agreements). But the actual decision of which network to connect to is made by the device itself, following a process defined by international standards.

This process is called PLMN selection (Public Land Mobile Network selection) and is defined in 3GPP specification TS 23.122. Every mobile device in the world follows this standard. It is not something that a SIM provider can override or customise.

The selection priority order

When your device is looking for a network to connect to – for example, when you arrive in a new country, switch your device on, or lose and regain coverage – it follows a strict priority order. This is the actual sequence defined by the 3GPP standard:

- Step 1: Your device looks for its home carrier network first. For example, a SIM issued by EE, it looks for EE.
- Step 2: Networks treated by the home carrier as equivalent to itself (e.g., sub-brands on the same infrastructure).
- Step 3: Networks the user has manually added as preferred, in priority order.
- Step 4: Networks the SIM provider has set as preferred via the SIM's stored list. This is where multi-network eSIM roaming agreements come into play.
- Step 5: Remaining available networks the device is permitted to use. If multiple networks are available at equal priority, the device selects at random, not by signal strength.
- Step 6: Signal strength is considered only here, as a simple pass/fail threshold. If no list-based selection has succeeded, the device will connect to any network with a detectable signal. This step is almost never reached for multi-network eSIMs with broad roaming agreements.

At Step 5, if your device has several permitted networks available and none has a higher list priority than the others, the device chooses between them at random. This means that in a location with three available networks – one with excellent signal, one with good signal, and one with marginal signal, your device is equally likely to connect to any of the three, provided all three meet the minimum signal threshold.

Signal does play one role: a simple pass/fail test. Can the device hear this network well enough to register? If yes, it is eligible. If no, it is excluded. There is no ranking, no comparison, no 'best signal' logic in the standard selection process. A network with one bar of signal is treated identically to a network with full bars, as long as both pass the minimum threshold.

Cell tower handover vs network switching

To understand why the 'best signal' claim does not hold up, it helps to understand the two fundamentally different ways a device can change its connection – and why one is seamless, and the other is not.

Seamless cell tower handover only works between towers on the same network. Vodafone hands you off between Vodafone towers. EE hands you off between EE towers. The network knows you, knows your session, knows your IP address, and coordinates the handover without interruption. This is possible because you are already authenticated and registered on that network.

Switching between carrier networks is nothing like this. Your device must completely disconnect from Vodafone, then connect to EE as if it were a brand-new subscriber arriving on EE's network



for the first time. It is not seamless. It takes time and every active data connection is interrupted during the process.

What this means for multi-network eSIMs

The "best signal" claim implies that a multi-network eSIM enables your device to continuously compare signal strength across multiple carrier networks and switch between them in real time. This does not happen, and for good reason: it would destroy the user experience rather than improve it. Imagine your phone disconnecting and reconnecting to a different carrier every few hundred metres - your call would drop, your video would buffer, your email would fail.

The real advantage of a multi-network eSIM is access and choice. Once connected to a network that is working, your device stays on that network and benefits from seamless cell tower handover within it – exactly as designed. You only need to switch to a different network when the current one stops working. The value is having the choice of networks to switch to when you need one, not constantly switching between them.

The standards body's own confirmation

The most authoritative confirmation that signal strength is not part of standard network selection comes from 3GPP itself.

In 2024, 3GPP introduced a new standard in Release 18 called SENSE – Signal level Enhanced Network SElection. SENSE was created specifically to add signal strength awareness to the network selection process, because the existing process does not have it.

"During the initial steps of selecting a network after switch-on or recovery from the loss of coverage, and during all steps of periodic re-selection, the signal level of available cells is not considered; solely the cell selection criteria as broadcast by the PLMN and the priority of networks are considered."

The very existence of SENSE proves the point: if the existing standard already selected the "best signal," there would be no need to create a new standard to add this capability. SENSE is new, designed primarily for stationary IoT devices, and not yet widely deployed in commercial smartphones or tablets.

What actually matters when choosing a multi-network eSIM

If 'best signal selection' is not a real differentiator, what should you be evaluating? Based on how network selection actually works, these are the factors that genuinely affect your connectivity experience:

1. How many networks does the eSIM give your device access to? This is the single most important factor. The more networks your device is permitted to connect to, the higher the probability that at least one of them has coverage in your specific location.
2. How quickly can you switch to the backup network when you need it? When your primary carrier has no coverage, you need to switch to your backup network fast.
3. What visibility and controls come with the connection? Once connected, what can you see and manage?
4. Is the provider honest about what their technology does? Technical credibility matters, particularly for enterprise procurement. A provider that makes claims unsupported by the governing standards is a provider you should evaluate carefully. The real value of a multi-network eSIM is network diversity and resilience, not a marketing claim about 'intelligent' signal selection.

Questions to ask any eSIM provider

When evaluating multi-network eSIM solutions, ask any provider - including us - the following questions:

1. "How does the SIM know which network has the strongest signal without connecting to each one first?"

If a provider claims 'best signal selection', this is the question that reveals whether the claim is technically supportable. A device cannot measure a network's signal without first disconnecting from its current network and registering on the new one - a process that takes seconds to minutes and interrupts all data sessions.

2. "Does the SIM or the device control network selection?"

The answer, per 3GPP standards, is always the device. The SIM defines which networks are permitted; the device's modem runs the selection algorithm. Any provider claiming their SIM 'controls' selection is either using imprecise language or misrepresenting the technology.

3. "How many carrier networks does your eSIM provide access to in the countries we operate in?"

This is the question that matters. Network diversity - the number of permitted networks available to your device - is the genuine differentiator between providers. More permitted networks means a higher probability of connectivity in any given location.

4. "What happens during a network switch? How long does it take? Are data sessions interrupted?"

Any honest provider will confirm that switching between carrier networks requires a full disconnection and reconnection, and that data sessions are interrupted. If a provider suggests their switching is seamless or instantaneous, ask them to explain the technical mechanism.

This month's top product picks

Here's a peek at some of latest new products...

Logitech introduces Signature Comfort Plus Lineup



LOGITECH has expanded its Signature Series with the launch of Signature Comfort Plus, a new mouse-and-keyboard lineup designed to make long desk days more comfortable for modern workers balancing professional and personal tasks. The range introduces the company's first cushioned palm support mouse and a keyboard with a dual-foam palm rest and curved typing angles, aimed at reducing strain during extended use.

The new products include the Signature Comfort Plus M850 L mouse, the MK880 keyboard-and-mouse combo, and the M840 L mouse variant without the palm cushion. Logitech says the lineup is built for "long, full days at the desk" where users frequently switch between devices, applications and moments of personal use. The tools are designed to minimise friction through quieter operation, simple controls and multi-device connectivity.

Art O'Gnimh, General Manager of Logitech's Mice & Keyboard Solutions Group, said the products are intended to support smoother daily workflows. "People now spend long, full days at their desks, constantly moving between tasks, screens, and personal moments," he said. "These are tools that don't ask for attention; they give it back, removing small distractions and adding comfort so everything feels smoother and more effortless."

The M850 L mouse debuts Logitech's palm cushion support, paired with a sculpted right-hand shape and rubber side grips. Logitech says the cushion has been tested with professionals to reflect real-world desk habits. The MK880 combo adds deep cushioned keys, a dual-foam palm rest and curved typing angles, with adjustable tilt options of 0°, 4° and 8°. Both devices feature silent clicks or lower-noise typing, SmartWheel precision scrolling, Easy-Switch connectivity for up to three devices, and customisable controls through Logi Options+.

A business-focused version is also available, equipped with Logi Bolt secure wireless connectivity and support for Logitech Sync, the company's device management platform. This allows IT teams to monitor device and firmware status across fleets, with multi-OS compatibility and quiet operation aimed at hybrid and shared workspaces. Logitech notes that enterprise models are designed for global deployment with customer support and long battery life to reduce maintenance.

Sustainability features include the use of 49–77% certified post-consumer recycled plastic, depending on colour, FSC-certified paper packaging and multi-year battery performance. Logitech says these measures support its Design for Sustainability principles and help lower the products' carbon footprint.

Captivate your audience with the Logitech Spotlight 2 advanced presenter



LOGITECH has introduced the Spotlight 2, an advanced presenter designed to help speakers deliver more confident and engaging presentations in hybrid and in-person environments. The device adds haptic feedback, digital highlighting tools and a force-sensitive interface to the familiar presenter format, aiming to support users before and during their time on stage.

The Spotlight 2 incorporates subtle tactile cues to guide presenters as they highlight slide details or follow a built-in breathing exercise intended to steady nerves. Logitech says the haptics are engineered to help speakers regulate their breathing and maintain focus, offering reassurance without diverting attention from the audience. The presenter's design centres on natural control, with a secure grip and an interface that allows the thumb to locate the main button instinctively.

Digital highlighting is a core feature of the new device. Spotlight 2 goes beyond traditional laser pointers by offering effects such as Spotlight, Magnify, Squarelight and Annotation, alongside a Digital Pointer and Class 1 laser. These tools are intended to help presenters emphasise key points clearly, whether addressing a room or a remote audience. Logitech positions the device as a way to ensure important information lands with impact, particularly in settings where clarity and precision are essential.

Users can tailor the presenter to their own workflow through the Logi Options+ app. The Action Button can be customised to trigger shortcuts including start, blank screen or mute, turning the device into a personalised control hub rather than a simple clicker. Logitech says this flexibility allows presenters to streamline their delivery and reduce reliance on the laptop during a talk.

Sustainability also features in the product's design. Spotlight 2 uses aluminium produced with renewable energy and certified post-consumer recycled plastic, with 43% recycled content in the plastic parts of all colour variants. Packaging is made from FSC-certified paper, contributing to a lower overall carbon impact.

The presenter offers Bluetooth pairing or connection via the included Logi Bolt USB-C receiver, a wireless range of up to 30 metres and cross-platform compatibility with PowerPoint, Google Slides and Keynote on macOS and Windows. A quick-charge function provides three months of use from a full charge or three hours of presentation time from a one-minute top-up. Logitech says the improved grip design ensures the device remains secure in hand, allowing presenters to stay focused on delivery rather than equipment.

Logitech launches Mobi Fold, its first ultra-portable foldable mouse for life on the go





LOGITECH has introduced Mobi Fold and Mobi Fold for Business, a new foldable mouse designed to support professionals who work between locations. The device aims to remove the friction that prevents many people from using a mouse outside traditional office settings.

Logitech's research highlights a clear gap in mobile working habits: although 72% of professionals own a mouse, only 26% use one in public spaces. The company attributes this to the bulk and inconvenience of conventional designs, which discourage use in cafés, airport lounges and other transient environments. Mobi Fold is intended to address this "On-the-Go Productivity Gap" by offering a compact device that folds to nearly half its size.

Joseph Mingori, VP and General Manager at Logitech, said the product was engineered to make mobile working more comfortable and consistent. He noted that users often leave their mouse behind not through preference, but because it is impractical to carry. According to Logitech, Mobi Fold reduces muscle strain by 22% compared with a laptop trackpad, providing a more ergonomic option for extended work sessions.

The device features a folding mechanism that powers the mouse on when opened and switches it off when closed. Adaptive Touch Scrolling supports both precise navigation and fast movement through long documents, while two touch-panel buttons can be customised through the Logi Options+ app. Mobi Fold connects with up to three devices via Bluetooth and is compatible with Windows, macOS, ChromeOS, Android, iPadOS and Linux. Quiet-clicks are included to minimise disruption in shared spaces.

Durability is a core part of the design. The mouse is drop-tested, wrapped in a dust-resistant silicone sleeve and built around a hinge rated for 15 years of daily use. A one-minute charge delivers up to 22 hours of operation, with a full charge lasting as long as 30 days. Logitech has also integrated an on-device AI model to help prevent accidental clicks during folding, and the product is the company's first input device to receive Google Fast Pair certification.

Three colour options—Graphite, Lilac and Off-White—are available globally. The device incorporates post-consumer recycled plastic and recycled rare earth magnets, and ships in FSC-certified paper packaging.

Mobi Fold for Business adds a Logi Bolt USB-C receiver, a two-year limited hardware warranty and Sync support for IT teams managing fleets of devices.

Omada unveils Fusion Gateway



OMADA, TP-Link's business solutions brand, has launched its Fusion Gateway product line, a new generation of integrated networking devices designed to streamline deployment, improve network performance and reduce the operational burden on small businesses. Announced in London on 15 June, the range targets restaurants, retail stores, offices and other SMB environments that often operate with limited IT support.

At the centre of the Omada ecosystem, Fusion Gateway provides unified management for Omada-connected devices across multiple sites. The new line is positioned as a significant upgrade for distributed businesses, enabling faster rollout and more efficient maintenance while improving overall network reliability.

The first products in the series are Fusion 2.5G, Fusion G+ and Fusion 2.5G PoE, each designed to support different deployment requirements. Fusion 2.5G includes a built-in controller offering licence-free cloud management, allowing users to monitor, configure and troubleshoot networks remotely via the Omada Cloud portal or app. This approach removes the need for device licences and reduces ongoing management overheads.

Setup has been simplified through Bluetooth onboarding and automatic discovery of Omada devices, enabling batch adoption to speed up installation. The gateway supports desktop, wall and rack mounting to suit varied environments.

Fusion 2.5G is powered by a quad-core CPU and features five 2.5G ports, up to four-WAN load balancing with auto failover, and advanced IDS/IPS. According to Omada, this delivers reliable, high-speed connectivity with VPN performance up to five times faster than comparable products. A 2.51-inch touchscreen provides real-time visibility into device status, traffic and diagnostics, reducing the need for laptops during on-site troubleshooting.

The new Omada LightLink VPN offers secure, one-click remote access via an invite link, allowing remote staff or branch locations to connect through the app or web interface. Additional software capabilities include multiple VPN protocols, optimised ACL and QoS, and full-mesh SD-WAN for distributed networks.

Ben Allcock, VP of B2B at TP-Link UK&I, said businesses are facing increasingly complex networking environments that demand time and IT capacity. He said the Fusion Gateway range enables networks to be managed from a single unified location, improving efficiency and supporting uninterrupted daily operations.

Omada also announced plans for the Fusion Pro series, aimed at more advanced multi-site environments. The Pro range will support integrated management of networking and surveillance devices, including Omada and VIGI products, offering a single-vendor ecosystem to simplify deployment and reduce ownership costs.

Omada's broader portfolio spans gateways, switches and Wi-Fi 7 access points, with the ecosystem expanding to include cameras and NVRs to support unified management across networking and surveillance.

3-in-1 wireless charging with Qi2

VERBATIM has expanded its mobile power range with the Charge 'n' Go Qi2 Power Bank, a compact unit designed to charge up to four devices at once. The new model combines magnetic Qi2 wireless charging with USB-C fast charging and comes in 5,000mAh (Grey) and 10,000mAh (Grey and White) capacities.

Supporting the latest Qi2 wireless charging standard, the Charge 'n' Go delivers up to 15W to compatible smartphones, with magnetic alignment ensuring accurate positioning. It works with MagSafe-enabled iPhones and other Qi2-certified devices, while Android users can benefit when using a magnetic case or ring. The power bank can also wirelessly charge an Apple Watch at up to 2.5W and wireless earbuds at up to 3W. A USB-C port enables a fourth device to be charged simultaneously.

For wired charging, the unit supports USB Power Delivery 3.0 with PPS and Quick Charge 3.0, delivering up to 20W on the 5,000mAh version and up to 30W on the 10,000mAh model. The bi-directional USB-C port can recharge the power bank itself or power connected devices.

A folding stand supports smartphones in portrait or landscape mode, while the compact ABS and aluminium alloy housing incorporates an LED battery indicator and six protection systems for safe operation.



Life in the channel

KASEYA LEANS INTO AI REALITY

Kaseya is accelerating hard into an AI-first future, reshaping its platform, security stack and partner strategy as MSPs face surging autonomous attacks and rising customer demand for guidance. **Dermot McCann, Executive Vice President and General Manager for International**, sat down for a catch-up with **PCR's Lynn Sencicle**.

When I last sat down with Dermot two years ago, the industry was already evolving under the weight of automation, consolidation and rising security pressures. But meeting him again at Kaseya's recent customer event at the London Museum in Docklands made one thing immediately clear: the pace of change has accelerated beyond anything the channel has previously had to absorb. AI is no longer a future-leaning talking point. It is the centre of gravity around which Kaseya is now building its platform, its internal operations and its expectations for MSPs.

The event itself was a lively, packed affair, with partners from across the UK filling the room long before Dermot took the stage. Before the keynote, I caught up with him for a conversation that was intended as a simple update on 'what's changed since we last spoke in August 2024', and it quickly became obvious that almost everything has.



Dermot didn't hesitate. "I have to start talking about AI," he said, "because that is the biggest change – it's moved beyond hype into reality." AI is no longer an optional enhancement or a speculative investment. It is now the defining force shaping Kaseya's roadmap, its customer expectations and the threat landscape MSPs must defend against.

The AI pivot inside Kaseya

Kaseya's internal transformation is perhaps the most striking change since our last conversation. The company has invested heavily in AI across three fronts: how partners use it, how Kaseya itself uses it, and how the platform is being rebuilt to operate in an AI-driven world.

Internally, AI is now embedded across service management, development and operations. Dermot described a company-wide shift involving 5,000 employees and a complete rethinking of workflows. The results are already visible where Kaseya has seen a 36% drop in service management tickets, driven partly by product improvements but also by AI-powered triage and automation. "We've leveraged our agentic AI inside our own service desk," he explained, "and it's ensuring that customer experience is sharper, faster and more consistent."

The development side has also been transformed. Kaseya committed to delivering 100 new features across the platform in a six-month period – it delivered more than 600. AI-assisted development is now standard practice, accelerating release cycles and allowing the company to respond to partner feedback at unprecedented speed.

The company has also expanded its global footprint to support this AI-first strategy. Investment in Krakow continues, a new

workflow-focused acquisition in Stockholm has been completed, and Kaseya has opened a Silicon Valley office to bring in "the best and brightest minds" in AI. Hundreds of millions of dollars have already been poured into the platform's next phase.

The threat landscape MSPs now face

The other side of the AI coin is security. Dermot was blunt about the scale of the challenge. "AI-assisted cyber-attacks are up 72% year on year," he said. "AI-generated phishing is four times more effective than traditional attacks." It is happening now, at scale, and MSPs are already feeling the pressure.

"Our biggest threat is autonomous attacks," he said. "That's a hacker's dream." Brute-force attacks can now be automated at a pace and volume that human teams cannot match. Kaseya's response is to build AI-powered defensive capabilities into its SOC, MDR and SIEM offerings.

The company's close relationship with the FBI and its compliance strategy – SOC 2, PCI, GDPR, EU Cyber Acts, NIST frameworks – are now central to its differentiation. As Dermot put it, "trust is the differentiator now in this space." With new AI-first vendors emerging rapidly, Kaseya is positioning itself as the secure, compliant alternative that can scale without exposing MSPs to unnecessary risk.

What MSPs are asking for now

The conversation turned to partners and how they are coping with the AI shift. Some are embracing it, some are resisting, but all are being pushed by their customers to provide guidance. "Their customers are all asking them, 'What does AI mean for our business?'" Dermot said. MSPs are being forced into more consultative roles, even as they maintain the traditional expectation that systems remain secure, available and well-managed.

This is where Kaseya's compliance management platform comes in. The company has released new versions aligned to the NIST AI Risk Management Framework and the UK Cyber Essentials 3.3 standard. Only 15% of MSPs currently offer compliance services, yet 70% of their customers need them. Kaseya sees this gap as one of the biggest opportunities for MSPs to evolve their business models.

The company announced its MSP Success programme in June, a business-coaching methodology designed to help partners reposition themselves for AI-driven consulting while still delivering profitable managed services. Dermot described it as a necessary shift: "The traditional MSP model has to change. It is more AI-focused, more consultative."

Digital specialists and agentic AI

One of the most significant innovations Kaseya is preparing to roll out is its 'digital specialists' – agentic AI workers embedded across the platform. These AI agents will automate repetitive tasks, triage issues, drive workflows and free engineers to focus on higher-value consulting work.

Partners involved in early testing have reported productivity improvements of more than 50%. Dermot emphasised that this is not about replacing humans. It is about hiring "a different type of human" and giving them tools that scale. "If we start automating functions that are not robust," he said, "then you're automating the problem." The focus is on strengthening the underlying platform first, then layering automation on top.

Dermot emphasised the idea that Kaseya's platform – not individual products – is now the core differentiator. MSPs often spend £24 per endpoint across multiple vendors. Kaseya's 365 platform, with AI-powered SOC included, comes in at around £3 per endpoint. "They're now thinking the platform is the differentiator, not the product," he said.

But the platform must still deliver best-of-breed products. Dermot was clear that Kaseya's SOC must be as strong as any competitor's, its AI strategy must be robust, and its workflow automation must be industry-leading.

Inside the event

When Dermot stepped on stage to open the event, he joked about "AI bingo" and warned the audience he would probably mention AI "150,000 times". He wasn't far off, but the humour sat alongside a serious message: Kaseya is investing heavily, moving fast and expects partners to do the same.

He spoke candidly about invoicing challenges, internal transformation, product quality improvements and the pace of development. He highlighted the 600 features delivered in a single quarter, the 12% drop in support tickets, and the major upgrades across remote control, EDR, device management and AutoTask.

His closing remarks, that "this AI revolution… it is beyond the hype, we are living and breathing it every day," captured the urgency and the scale of what Kaseya believes is coming next: AI across the entire security suite, AI across the entire platform, AI powering defensive strategies, reporting, automation and service delivery.

MSPs are being pushed into a new era where consulting, compliance, automation and cyber resilience must sit alongside traditional managed services, and Kaseya is positioning itself as the partner that can help them make that leap securely, profitably and at scale.



PCR AWARDS

WEDNESDAY 21ST OCTOBER 2026 | GRAND CONNAUGHT ROOMS - LONDON

BOOK YOUR TICKETS!

DON'T MISS OUT



For sponsorship opportuniities, contact:
dtucker@datateam.co.uk

Supporting sponsor:

QBS SOFTWARE DELIVERY PLATFORM

Proud sponsor:

AOC

CI DISTRIBUTION

ebay

WESTCOAST Powered by ALSO

brother
at your side



Still think offering more than hardware is a hard sell?

86% of your customers prefer print on a contract*

Customers want managed print services (MPS) – but some resellers prefer to just sell them a device. Offering MPS doesn't have to be complex – with the right vendor "At your side", it's simple to win new deals, retain customers and grow your business.

Brother MPS is simple, scalable and here to help you meet customer demand.

- Increase profitability versus hardware-only sales
- A range of MPS options
- Increase customer life-time value
- More upsell opportunities
- Ongoing support from Brother

Brother MPS Makes Printing Simple

Managed Print Services

Source: IDC Survey Spotlight: How Do Current Print Contract Arrangements Among European Enterprises Compare with Their Preferred Engagement Models?, #EUR154530626, June 2026

Grasp the MPS opportunity – learn more on BrotherZone

Brotherzone.co.uk/make-printing-simple