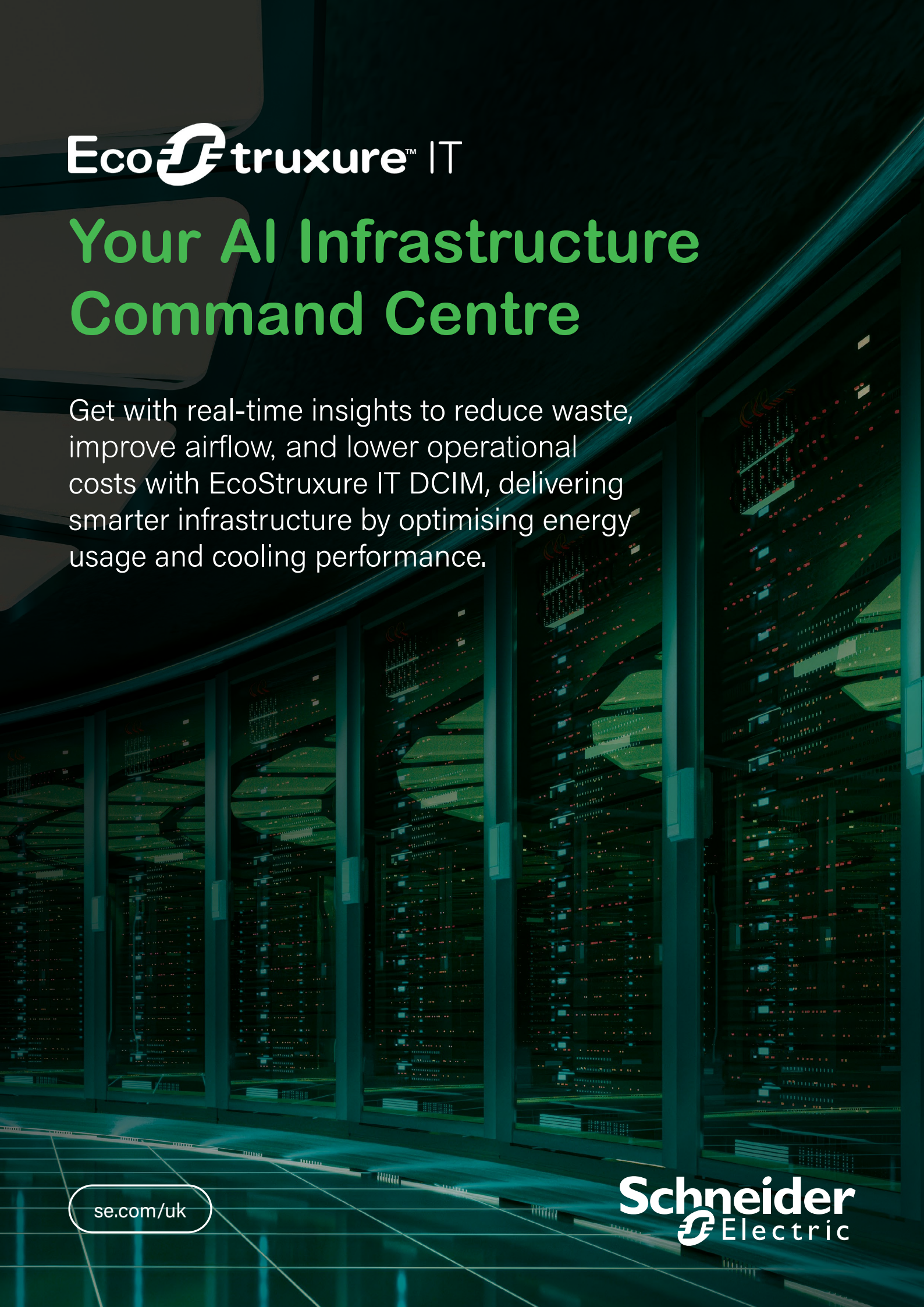
MSP CHANNEL INSIGHTS

ISSUE IV 2026

AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

MSP-CHANNEL.COM

THE HIDDEN HUMAN COST OF CYBERSECURITY BURNOUT


EcoStruxure™ IT
Your AI Infrastructure Command Centre
Get with real-time insights to reduce waste, improve airflow, and lower operational costs with EcoStruxure IT DCIM, delivering smarter infrastructure by optimising energy usage and cooling performance.
se.com/uk
Schneider Electric

VIEWPOINT

BY SOPHIE MILBURN
EDITOR

Digital workers, human limits and the new strain at the heart of cybersecurity

IN CYBERSECURITY, two forces are colliding: the rapid expansion of autonomous digital systems and the growing strain placed on the people expected to govern them. What once looked like a story of technological efficiency is increasingly becoming one of organisational overload, where speed is no longer a competitive advantage but a source of sustained pressure.

On one side, organisations are quietly building something new: a digital workforce. Not just tools that assist humans, but autonomous systems that act, decide, and operate continuously inside business environments. They process information and move across systems at a speed no human team could match alone. It feels like progress. And in many ways, it is.

But on the other side of that progress sits an uncomfortable reality. Responsibility has not automated itself.

Security teams are still expected to understand what all of this activity means, decide what matters, and step in when something does not look right. Only now, they are doing it in an environment where the noise has multiplied, the pace has accelerated, and the actors involved are no longer just human or machine, but something in between.

That shift changes everything, even if it has not fully been named yet.

Because when systems start acting independently, security stops being about monitoring tools and starts becoming about supervising behaviour. And when behaviour scales faster than understanding, pressure follows quickly behind.

You can see it in the rhythm of the job. The constant pull to stay alert just a bit longer. The habit of checking things “one more time.” The feeling that stepping away might mean missing something critical. Over time, that does not just create busy teams. It creates tired ones. Not dramatically exhausted in a single moment, but steadily worn down by never quite reaching “done.”

And yet, the expectation of accountability has not eased. If anything, it has tightened. When something goes wrong, the natural instinct in many organisations is still to look for a point of human failure, even when the reality is far more distributed. Systems are complex, decisions are layered, and outcomes are rarely the result of a single action. But pressure tends to simplify that story anyway.

This is where the real tension sits. We are scaling automation faster than we are redesigning responsibility. We are adding digital actors into the environment without fully rethinking what it means to oversee them.

The answer is not to slow innovation down. That much is unrealistic. But it does require a shift in mindset. From expecting control to designing collaboration. From treating automation as something to supervise, to treating it as something to work alongside. And critically, from assuming humans will simply “keep up,” to acknowledging that sustainable performance has limits.

Because the future of cybersecurity will not be defined by how autonomous systems become. It will be defined by whether the people responsible for them can still think clearly, act decisively, and just as importantly, step away when they need to.

Contents

Cover Feature

The hidden human cost of cybersecurity burnout

This article explores the growing human impact of cybersecurity work, drawing on an exclusive podcast with Anna Webb, Global Director of Security and Identity Support Services at Kocho, alongside new research highlighting the levels of stress, pressure, and job insecurity experienced by senior cyber professionals across the UK.

18 Scaling without sacrifice at Chorus

Based on an exclusive interview with Nicola Saner, CEO of Chorus, this article takes a behind-the-scenes look at how the MSP is scaling in a fast-changing market, and the thinking behind its approach to growth, service delivery, and long-term customer relationships.

22 AI tools to digital employees: Why traditional security models are falling behind

Exploring how the rise of the digital workforce is reshaping cybersecurity.

26 Technician to leader: The art of letting go

In an exclusive podcast discussion, Craig Sharp, Owner and Founder of Abussi, shares his journey from hands-on IT technician to business leader, highlighting how growth requires letting go of day-to-day tasks and trusting others.

30 Guardz Q&A: Agentic AI, strategic partnerships and building MSP-first security platforms

In this Q&A, Doni Brass, SVP Product Strategy & Community at Guardz, discusses how MSPs are adapting to rising cyber threats, the shift toward platformisation, and how AI-driven automation and strategic partnerships are reshaping security delivery for small and medium-sized businesses.

34 DigiCert Q&A: AI threats, certificate lifecycle risk and channel strategy

In this Q&A, Christian Stanford, RVP EMEA Channels at DigiCert, discusses the company's channel-first strategy, the growing urgency around certificate lifecycle management, and how partners can help organisations navigate AI-driven security risks, compliance demands and emerging threats such as quantum computing.

36 How channel partners are managing overconfidence in AI controls

As AI adoption accelerates, many organisations are discovering a growing gap between visibility and control. For MSPs and MSSPs, helping customers manage AI risk is emerging as both a security challenge and a strategic opportunity.

38 Cognitive enterprises, autonomous firms, platformisation, and trust as a service are poised to shape the future of work

AI is reshaping work and business models, but future success will depend on how organisations harness human knowledge.

40 The hidden barrier to scaling a SOC: consistency, not technology

As MSSPs scale, maintaining consistent investigative quality becomes increasingly difficult. In complex SOC environments, long-term success depends not just on tools and automation, but on embedding context, judgment and trust into day-to-day operations.

42 Why digital transformation strategies fail in delivery - not design

Why do so many transformation programmes lose momentum after a strong start?

44 The sovereignty gap UK organisations can no longer afford to ignore

Cloud strategy is entering a new era, shaped by sovereignty, resilience and geopolitical risk.

46 Your security stack might be your biggest vulnerability

Complex security stacks can weaken protection. The future for channel partners lies in simpler, resilient architectures focused on control, containment and outcomes.

NEWS

06 Pax8 and NinjaOne forge alliance to enhance SMB security

07 LevelBlue & SentinelOne forge alliance for enhanced security operations

08 NinjaOne strengthens backup with unified IT operations platform

09 SonicWall reveals 2026 cyber protect report

10 UK's small business leaders embrace AI for growth

11 The growing fault line: AI tools and employee disengagement

12 Trust and resilience: The cornerstones of AI and data security

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

Consulting Editor
Philip Alsop
philip.alsop@angelbc.com

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

Sales Manager
Peter Davies
+44 (0)1923 690211
peter.davies@angelbc.com

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

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

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

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

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

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

Directors
Sukhi Bhadal: CEO
Scott Adams: CTO

Angel BUSINESS COMMUNICATIONS

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

ISSN 2396-9016 (Online)

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

Pax8 and NinjaOne forge alliance to enhance SMB security

Pax8 teams up with NinjaOne, aiming to strengthen managed service providers through enhanced solutions and security infrastructure for SMBs.

PAX8, a global AI and cloud marketplace focused on small and medium-sized businesses (SMBs), has announced a partnership with NinjaOne. The collaboration is intended to support managed service providers (MSPs) and managed intelligence providers (MIPs) by providing solutions aimed at supporting growth and strengthening security capabilities in an evolving AI landscape.

The partnership is expected to support efficiency improvements and user experience, alongside developments in security capabilities. SMBs are frequently targeted by cyber attacks, making security a key consideration for this segment.

Under the agreement, Pax8 will introduce MSPs and MIPs seeking unified IT operations to NinjaOne, which specialises in remote monitoring and management (RMM).

The partnership is expected to support efficiency improvements and user experience

NinjaOne will be responsible for ongoing partner engagement and managing the customer lifecycle, while Pax8 will continue to identify opportunities and provide strategic guidance.

The collaboration builds on an existing relationship involving Dropsuite, following NinjaOne's acquisition of the SaaS backup and archiving provider in 2025. It is intended to expand the range of technology solutions available to MSPs and MIPs, in the context of NinjaOne's growth in the RMM market.

According to Pax8's research report, 'Pulse', 84% of small businesses indicate a willingness to rely on external technology advisors for AI implementation, highlighting the role of MSPs and MIPs in supporting SMBs in this area.

The Pax8 and NinjaOne partnership operates globally, with regional contact points across North America, EMEA and APAC. The structure is designed to support MSPs and MIPs across different regions and provide access to technology solutions for business operations.

LevelBlue & SentinelOne forge alliance for enhanced security operations

LevelBlue has partnered with SentinelOne to deliver AI-driven security solutions, aimed at enhancing detection and response capabilities.

LEVELBLUE, a provider of managed security services, has entered into a global strategic partnership with SentinelOne, a company specialising in AI security. The collaboration is focused on delivering integrated, intelligence-driven security operations across organisations globally.

The partnership combines SentinelOne's AI capabilities, including its Purple AI and Singularity Platform, with LevelBlue's threat intelligence-led operations and Indigo security platform. The aim is to improve visibility, accelerate detection, and support response in complex digital environments.

Under the partnership, LevelBlue will act as a preferred global partner provider for SentinelOne, delivering managed detection and response (MDR) and managed security information and event management (SIEM) services. The relationship also includes incident response (IR), supporting organisations in preparing for, responding to, and recovering from cyber incidents.

The collaboration is intended to integrate AI-driven detection with human-led investigation and response. This approach is designed to reduce dwell time, improve remediation speed, and support cyber resilience. It also integrates SentinelOne's SIEM analytics with LevelBlue's Indigo platform to support security operations across different environments.

SentinelOne provides data ingestion, normalisation, and analytics, while LevelBlue focuses on investigation, response, and service delivery. The combined approach is intended to address the challenge of linking detection with response.

The offering aligns telemetry across endpoints, cloud workloads, and identities, with continuous monitoring and analyst-led triage. This supports earlier detection of threats, coordinated response, and visibility across hybrid environments.

As part of the partnership, LevelBlue has a team of more than 300 digital forensics and incident response professionals. The team supports organisations in responding to cyber incidents, including ransomware, nation-state activity, and large-scale breaches. Its incident response services include CREST-certified teams and retainer-based engagement models.

OpenText expands European presence with AWS sovereign cloud integration

OPENTEXT, a company focused on secure information management for AI, has made its enterprise data and AI solutions available on the AWS European Sovereign Cloud. The aim of this initiative is to support secure and compliant data handling for organisations operating in Europe.

The Canadian-based company is integrating its hybrid sovereign cloud services with the AWS European Sovereign Cloud, making its services available to customers in the European market. This allows organisations to use AWS cloud capabilities while keeping data governance and residency within European boundaries.

The available suite includes OpenText Content Management, OpenText Documentum Content Management, OpenText Core Application Security, and OpenText Core Service Management. These tools are delivered through AWS's sovereign cloud infrastructure and support structured content management as well as preparation of data for AI-driven analytics and automation.

Customers can use these services while benefiting from AWS security standards, availability, and performance, as well as meeting European Union requirements related to operational autonomy and data residency.

The AWS European Sovereign Cloud is designed as an independent cloud environment with technical controls and legal frameworks intended for European governments and enterprises. Its infrastructure is located entirely within the EU and is separated from other AWS Regions.

Organisations using the platform have access to AWS services, security features, performance capabilities, and ongoing updates within a consistent architecture. AWS components such as the Nitro System are also available, supporting application development while maintaining customer control over data and operations.

NinjaOne strengthens backup with unified IT operations platform

NinjaOne Backup is gaining traction for its integrated IT management approach, offering backup capabilities aimed at improving efficiency and supporting data resilience.

NINJAONE has reported increased adoption of its NinjaOne Backup solution, which is used by over 15,000 customers. The tool is used to protect endpoints, servers, and SaaS applications, reflecting demand from IT teams and managed service providers (MSPs) for backup capabilities within a unified IT operations platform.

NinjaOne Backup supports device and SaaS data protection within the NinjaOne Unified IT Operations Platform. It includes backup options for applications such as Microsoft 365, Google Workspace, and Microsoft Entra, with automated backup functions intended to support compliance requirements and data recovery processes.

Recent updates to the product include:

- **Advanced Backup Engine:** A redesigned engine intended to improve storage efficiency, reduce resource usage, and increase backup speed, reducing manual intervention for IT teams and MSPs.
- **AI-Driven Verification:** The Boot Verify feature automates testing of backup image recoverability using AI in a virtual environment, supporting validation of backup integrity.
- **Expanded Compliance Features:** Includes backup retention options of up to 10 years, automated alerts for policy changes, and multi-factor authentication for selected operations.

"IT teams and MSPs have enough on their plates without having to manage backups as a standalone, siloed workflow," said Matt Hastings, SVP, Product Management at NinjaOne.

"NinjaOne Backup gives them time back with faster backups, less storage overhead, and simpler compliance. Our customers are already using that time to take on more clients and strategic work."

Through a single console, organisations can look to monitor backup status and manage recovery processes, with automation and controls supporting data protection and compliance requirements.

Advania UK strengthens leadership with key appointments

ADVANIA UK, part of Northern European IT services provider Advania Group, has expanded its leadership team with the appointments of Sabrina Harris as Chief Financial Officer and Tara Allison as Chief Marketing Officer. These appointments form part of the company's ongoing development in the UK market.

Since establishing a presence in the UK in 2021, Advania has grown its operations and service offering. This growth has included acquisitions such as Servium and CCS Media last year. The recent leadership appointments align with the company's focus on performance, market presence, and customer relationships.

Sabrina Harris joins from BT, where she held several senior finance roles, most recently working in commercial finance with global teams and complex customer contracts. She has experience in areas including profitability, financial governance, and supporting large-scale transformation in technology-focused environments.

Tara Allison brings more than 25 years of experience in B2B technology marketing. Her background includes work in brand development, demand generation, and commercial marketing impact. She previously held the position of marketing lead at Trend Micro across the UK and Ireland, where she worked across brand, demand generation, and sales alignment.

These appointments contribute to the company's ongoing development in the UK, with a focus on operational performance and market engagement as Advania continues to evolve its presence in the region.

Tara Allison brings more than 25 years of experience in B2B technology marketing. Her background includes work in brand development, demand generation, and commercial marketing impact

SonicWall reveals 2026 cyber protect report

SonicWall's latest report identifies the 'Seven Deadly Sins of Cybersecurity', focusing on protection outcomes crucial for small and medium-sized businesses (SMBs).

SONICWALL has released the 2026 Cyber Protect Report, shifting its approach from traditional threat reporting to a focus on protection outcomes for business leaders.

The report finds that many small and medium-sized businesses (SMBs) are affected less by complex cyberattacks and more by recurring, preventable gaps, identified as the Seven Deadly Sins of Cybersecurity. These issues are presented as key factors influencing levels of cyber resilience and exposure.

Drawing on data from a global network of more than one million security sensors, the report outlines trends in the threat landscape:

- High and medium severity attacks increased by 20.8% to more than 13 billion incidents
- Automated bots generate over 36,000 vulnerability scans per second, accounting for more than half of all internet traffic, with bad bot traffic representing 37% of global traffic
- Internet of Things (IoT) attacks rose by 11% to 610 million hits, while Log4j accounted for 824.9 million intrusion prevention system (IPS) hits in 2025
- Identity, cloud, and credential compromise account for 85% of actionable security alerts, with stolen passwords more commonly used than zero-day exploits
- SMBs experienced ransomware in 88% of breaches in 2025, more than double the rate seen in larger enterprises

The 2026 Cyber Protect Report is structured around protection outcomes rather than threat statistics alone. It identifies seven recurring operational issues, referred to as the Seven Deadly Sins of Cybersecurity:

- Ignoring the Fundamentals: Weak authentication and unpatched systems remain common vulnerabilities
- False Confidence: Overestimating security posture without validation can create gaps
- Overexposed Access: Permissive access controls and network configurations can allow lateral movement
- Reactive Security Posture: Limited monitoring and lack of proactive measures can delay detection
- Cost-Driven Security Decisions: Delayed investment may lead to higher long-term costs
- Reliance on Legacy Access Models: VPNs continue to be a commonly exploited entry point
- Chasing Hype Over Execution: Incomplete deployment of tools and processes can reduce effectiveness

The report is intended to support Managed Security Service Providers (MSSPs) in engaging with SMB decision-makers, helping to align technical threat data with business risk.

It concludes that differences in security outcomes are often linked to execution rather than technology alone, and is positioned as a resource for MSPs, MSSPs, and SMB organisations.

UK's small business leaders embrace AI for growth

A survey reveals that ambitious small business owners in the UK view AI as pivotal for their growth strategies.

AT THE RECENT "AI for Growth" event hosted by Goldman Sachs in Birmingham, nearly 300 high-growth small business owners gathered to discuss and share use of artificial intelligence (AI), highlighting its growing role in UK small business operations.

New data indicates that 98% of participants in the Goldman Sachs 10,000 Small Businesses UK programme are already using AI. Over half report improvements in operational efficiency, while 72% have seen increases in employee productivity.

The findings come from a March 2026 survey of over 400 programme graduates. Within this group, 19% report improved financial performance and a similar proportion report higher customer satisfaction and retention. Around 21% say they are yet to see measurable impact, often those at earlier stages of adoption.

AI is also increasingly embedded in business strategy. For 56% of respondents, AI is described as either essential or a significant part of future growth plans, while 4% say it does not form part of their strategy.

Recruitment approaches are also evolving. AI literacy is now a key hiring criterion for 24% of leaders surveyed. In addition, 85% of respondents said they would be open to hiring autonomous AI systems if available.

The results contrast with broader UK data, which suggests 35% of small businesses currently use AI. Within the 10KSB cohort, 89% report paying for AI tools compared with 33% in the wider market.

Beyond tool adoption, 38% of respondents have developed custom AI solutions for their businesses. AI is being integrated into core systems such as CRM, accounting, and HR platforms, with marketing remaining the most common use case. Around 19% of businesses report using agentic AI systems capable of autonomous decision-making.

These findings are based on a survey of 407 participants in the Goldman Sachs 10,000 Small Businesses programme, providing a snapshot of AI adoption and usage trends among UK high-growth SMEs.

The growing fault line: AI tools and employee disengagement

A gap exists between executive enthusiasm for AI and employee trust in these tools, alongside the use of unsanctioned AI applications.

CURRENT TRENDS in enterprise AI investment show high levels of financial commitment, but employee engagement with these tools remains limited. WalkMe's State of Digital Adoption report indicates that 54% of workers avoided using AI tools and instead completed tasks manually within the past 30 days, while a further 33% reported not using AI at all.

The survey, which included 3,750 executives and employees across 14 countries in enterprises with more than 1,000 employees, highlights a difference in perspectives between executives and employees within organisations.

On trust in AI, 9% of workers report confidence in AI for complex business decisions, compared with 61% of executives. On tools and resources, 88% of executives believe employees have adequate tools, while 21% of employees agree. Regarding productivity, 81% of executives report improvements linked to AI use, while employees report losing an average of 7.9 hours per week due to digital friction.

The report also notes an increase in time lost to technology-related issues. Workers now report the equivalent of 51 lost working days per year due to digital friction, a 42% increase compared to 2025. This follows a previous decline from 43 days in 2024 to 36 days in 2025. Despite a 38% increase in digital investment year-on-year, the report states that around 40% of this investment is not delivering expected outcomes.

The report also identifies increased use of unsanctioned AI tools. Around 45% of employees report using non-approved AI tools in the past 30 days, and 36% report using them with confidential data. While 78% of executives say they intend to address unsanctioned AI use, 21% of employees report being warned about AI policies.

Additionally, 34% of employees say they are unclear about which AI tools are officially approved. At the same time, 62% of executives believe concerns about unsanctioned "shadow AI" are overstated compared to the risk of underusing AI.

Atlassian introduces AI-powered 'Remix' for confluence

ATLASSIAN CORPORATION, known for its collaboration tools such as Jira, Loom and Confluence, has introduced new AI-driven features in its Confluence knowledge management platform. The updates are designed to support the transformation of content into visual formats while retaining context and reducing the need for manual reformatting.

A new feature, "Remix", currently in open beta, allows users to convert Confluence pages into visual outputs such as charts, infographics and presentation-ready summaries. Users can select content including paragraphs, tables or full documents and generate inline visuals. The feature also provides format suggestions based on content type and usage patterns within the Teamwork Graph.

Remix is designed to maintain a single source of truth by layering visuals on top of linked original content, without requiring exports or the creation of additional pages. At launch, it supports formats including data visualisations, infographics, scorecards and charts, with further formats planned.

Atlassian has also introduced third-party agents built on the Model Context Protocol (MCP), connecting Confluence with partner tools. The initial set of agents, launched on 13 April, includes:

- The Lovable Agent, which converts product specifications into UI prototypes
- The Replit Agent, which turns technical documents into starter applications
- The Gamma Agent, which transforms text such as meeting notes or status pages into presentations

These agents can be launched from Confluence, where they access page content and metadata and pass context into partner tools. The resulting outputs link back to the original Confluence page. The system is powered by Rovo and built on MCP, enabling Confluence content to be used across integrated tools while retaining context.

Atlassian states that setup is designed to be simple, with administrators able to enable partner MCP servers through Atlassian Administration, allowing agents to appear in the Rovo directory. The company plans to expand the range of partner integrations over time, further extending its AI-enabled ecosystem.

Trust and resilience: The cornerstones of AI and data security

Data resilience is increasingly viewed as important for organisations operating in the AI era, as executive concern over outages continues to grow.

VEEAM SOFTWARE has released its latest Data Resilience survey findings, highlighting growing concern around data loss and outages. In an environment where data and AI increasingly underpin business success, the need for resilient and secure data systems continues to grow. However, the findings indicate that many boards and executives are not yet fully prepared for risks associated with AI-driven threats.

The annual reminder on 31st March highlights that regular, reliable backups are a key component of digital trust and business continuity. Veeam's findings show that executive concern about outages now exceeds concerns about economic downturns. Ransomware is the most frequently cited threat, referenced by 67% of business leaders. AI-related risks such as data leaks and algorithm bias are ranked lower but are still considered relevant at board level.

Survey highlights include:

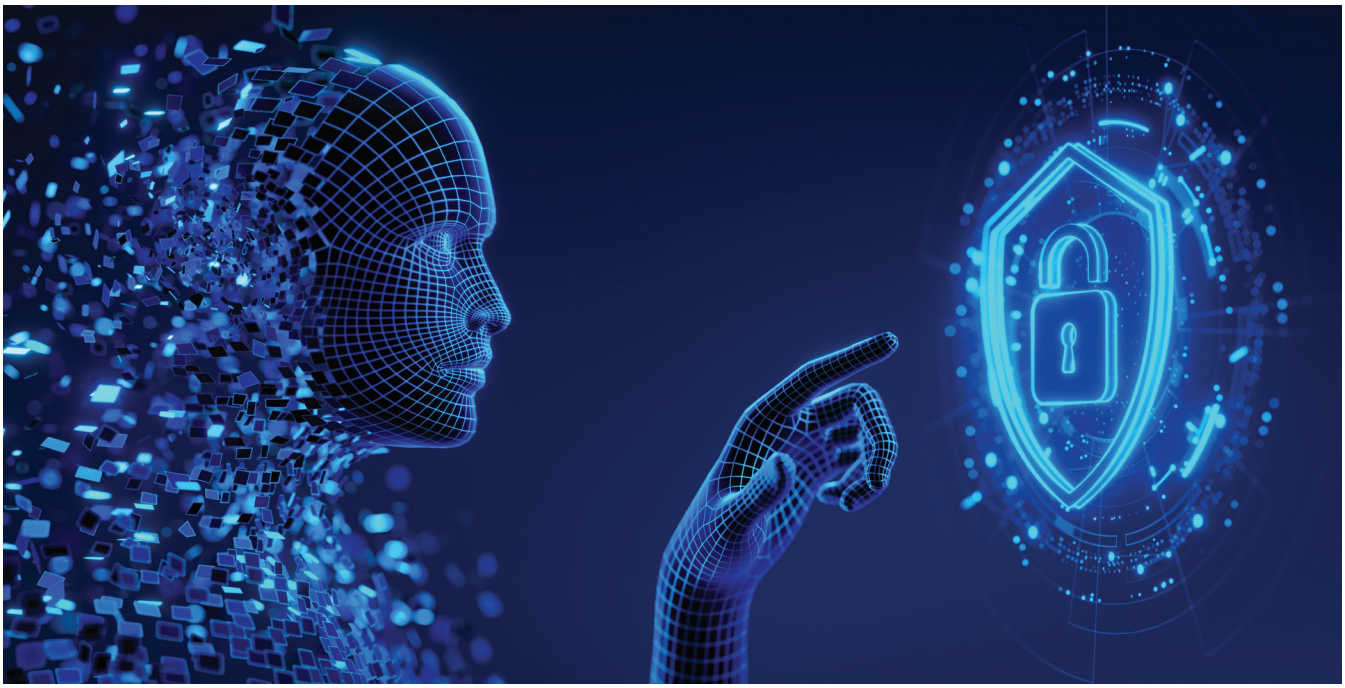
- 76% of organisations report they would struggle significantly if faced with a three-day data outage.
- Over 40% of IT leaders are not confident in their ability to recover critical data within 24 hours of a cyberattack or data loss event.
- The consequences of data failures include reduced customer trust, reputational damage, and regulatory penalties, and in some cases may threaten business continuity.
  As a result, data resilience is increasingly viewed as a core business consideration rather than solely an IT function.

Despite increasing use of AI, governance around AI risk and resilience remains limited. Only a minority of boards regularly assess recovery readiness, and responsibility for resilience is often distributed across multiple executive roles, which can contribute to more reactive approaches to risk management.

Additional findings from Veeam include:

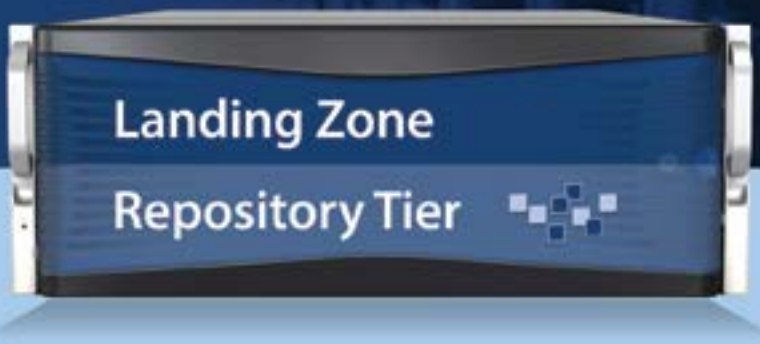
- Human impact: Major cyber incidents have been linked to employee resignations and burnout, highlighting the wider organisational effects of such events.
- Causes of data loss: External cyberattacks, human error, and system failures remain the most common contributors.
- Prevalence of outages: 83% of organisations report experiencing unresolved data outages in the past five years.

With World Backup Day approaching, organisations are encouraged to review, test, and strengthen their data resilience strategies. The consequences of gaps in resilience can include reduced customer trust, reputational damage, compliance challenges, and operational disruption.



EXAGRID
Tiered Backup Storage

The future is here.
Tiered Backup Storage



FASTEST BACKUPS

FASTEST RESTORES

SCALABILITY FOR FIXED-LENGTH BACKUP WINDOW

COMPREHENSIVE SECURITY WITH RANSOMWARE RECOVERY

LOW COST UP FRONT AND OVER TIME

MSP CHANNEL AWARDS
2025 WINNER

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

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

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

LEARN MORE >

The hidden human cost of cybersecurity burnout

This article explores the growing human impact of cybersecurity work, drawing on an exclusive podcast with Anna Webb, Global Director of Security and Identity Support Services at Kocho, alongside new research highlighting the levels of stress, pressure, and job insecurity experienced by senior cyber professionals across the UK.

THIS ARTICLE follows new Kocho research revealing the significant human strain within the cyber industry, with 84% of senior professionals fearing a serious breach could cost them their job, and over half reporting consistently high stress levels within their teams. Many also struggle to switch off outside working hours, highlighting the intensity of 'always-on' security roles.

While cyber incidents are often measured in financial and operational terms, the findings underline a less visible reality: the personal toll on the people responsible for defending critical infrastructure.

Insights from the exclusive discussion with Anna Webb bring this into focus, highlighting the lived experience behind the statistics, including the pressure, responsibility, and psychological burden carried by cybersecurity professionals in an environment shaped by constant threat and escalating complexity.

When cybersecurity becomes personal

One of the clearest themes to emerge from Webb's experience is that the pressure within cybersecurity is not simply operational; it is deeply personal. While infrastructure teams are often judged on uptime and recovery, she draws a distinction in how cyber teams are evaluated and perceived when things go wrong.

As Webb explains, infrastructure teams operate under significant pressure when systems fail or bugs occur, as they are expected to restore services quickly and get everything back up and running. However, in cybersecurity, the stakes shift from system recovery to public exposure and reputational fallout.

Anna highlights that the defining fear is often visibility rather than downtime, pointing to high-profile incidents such as recent retail breaches.

That visibility, she argues, creates a level of pressure that extends far beyond organisational impact. While financial consequences are widely understood, the personal and professional ramifications for individuals are often overlooked. "Nobody thinks about what that means reputationally for you as an analyst, as an engineer, as somebody actually running the department," she notes.

Perhaps most striking is her reflection on how a single incident can shape an entire career trajectory. "It's about that one day in time that can change your whole career," Anna explains, describing how even junior analysts may find themselves defined by a moment of failure in future job opportunities.

This contributes to a culture where highly skilled professionals carry sustained pressure without visibility or acknowledgement. As she puts it,

"I've spent a lot of my career watching incredibly capable people carry an immeasurable and impossible pressure in complete silence, because they know they've got to do this job day in, day out."

It is this silent burden, rather than the technical challenge alone, that defines much of the human reality of cybersecurity work.

Hypervigilance vs detachment

If the threat of a breach is ever-present, the way cyber professionals respond to that pressure can be just as defining as the incident itself. For the channel, where MSPs and security teams operate in 'always-on' environments, this tension is particularly evident.

Webb describes a clear split in behaviours, particularly among those who feel a constant sense of responsibility. As she explains, some professionals become almost hypervigilant, rarely switching off and remaining in a constant state of 'what if' thinking about potential threats. In practice, that means checking notifications late at night, logging in 'just to have a look', and never fully stepping away from the job. Even when there are solid processes and escalation paths in place, the instinct is still to keep one eye on things. This means switching off properly rarely happens, and without that downtime, there's no real chance to recharge.

At the other end of the spectrum, the same pressure can lead to emotional detachment. Webb highlights that some people take a very firm boundary approach, fully switching off once their shift ends and viewing anything outside of it as no longer within their responsibility. In the channel, this presents a different kind of risk. While clear boundaries are essential, disengagement can undermine accountability and team cohesion, particularly in smaller or stretched security teams.

For MSPs and security providers, this tension highlights a deeper challenge. It is not just about having the right tools or processes in place, but about building an environment where individuals can maintain balance without compromising performance.

Webb describes a clear split in behaviours, particularly among those who feel a constant sense of responsibility. As she explains, some professionals become almost hypervigilant, rarely switching off and remaining in a constant state of 'what if' thinking about potential threats

Encouraging openness in high-pressure environments

When it comes to whether these pressures are openly discussed, Webb points to a clear split in the industry. While some still hold back until things reach a breaking point, she notes that attitudes are shifting, with more professionals now willing to speak up earlier and say when they need time out.

She also reflects on how this is changing culturally, particularly in a space that has traditionally been male-dominated, where speaking about stress or mental health can still feel uncomfortable for some. But that perception is gradually shifting, with more openness emerging across teams.

For Kocho, Webb suggests this is something the organisation has actively tried to support. She highlights the importance of structured wellbeing support, from policies around mental health and annual leave to regular webinars and open internal conversations. In an industry where pressure is constant, that kind of environment can be the difference between silent strain and sustainable careers.

Blame culture and job security

In cybersecurity, pressure doesn't just come from the threat of attack itself, but from what happens afterwards. The sense that a single incident can define a career sits heavily in the background, shaping how people behave long before anything actually goes wrong.

Webb is clear that this concern is not unfounded: "your career is judged on your worst day, so if something happens that's quite significant, there is that sort of worry." In practice, that means professionals are not only managing systems and incidents, but also the potential career consequences of those incidents, which can include anything from reputational damage to demotion or job loss in more senior roles.

That pressure is felt differently across the industry and often comes down to internal scrutiny after an incident, particularly when teams are responsible for preventing exactly what has gone wrong. There is a tendency for organisations to look at what you have done in the aftermath, rather than stepping back to assess tooling, processes, and broader systemic factors.

At the same time, this can create a tension between hypervigilance and fear of failure. When people are constantly alert to potential

issues, there is still no guarantee of catching everything, especially in an environment where threats evolve quickly and AI is accelerating change. Yet if something is missed, even unintentionally, the personal stakes can feel disproportionately high.

This environment can ultimately push people towards silence rather than action. If raising a concern risks being associated with an incident, some may choose not to speak up at all. That hesitation has wider implications in the channel, where early visibility and fast escalation are critical to preventing issues from escalating.

The result is a culture where pressure and accountability can blur together. Effective security is not just about individuals or mistakes, but about people, process, and technology working in balance. When blame overshadows that balance, it becomes harder to build resilience across teams or to maintain confidence in the face of constant threat.

Building a healthier cyber culture

One of the clearest themes running through Webb's perspective is that pressure in cybersecurity is not just technical; it is cultural. Webb explains: "who you work with and who you work for makes a big impact." That framing matters, particularly for MSPs, where analysts and engineers are often operating across multiple clients and incident environments at once. In that kind of setup, the organisational tone set by leadership directly shapes whether teams feel supported when incidents happen, or exposed to blame when things go wrong.

Cybersecurity rarely offers clean, predictable outcomes, which is something MSPs are constantly dealing with in real time. It is not an exact science and things are changing constantly. For MSPs, that unpredictability is the operating reality, not the exception. Threats evolve quickly, visibility is fragmented across clients, and even well-run processes can be overtaken by events. Framing performance expectations around certainty, rather than volatility, is where pressure can start to become unfair.

That is why Webb draws a clear line between accountability and blame when incidents occur. There is a clear difference between negligence and the realities of working in cybersecurity today. Teams are operating in an environment where threats evolve rapidly and the pace of change, particularly with the rise of AI and increasingly sophisticated attack methods, makes it difficult to stay consistently ahead. In that context, incidents cannot always be reduced to individual failure. Much of the pressure comes from trying to defend systems that are shifting faster than processes and human response can reasonably adapt to.

Webb's wider message is that resilience in cybersecurity does not come from constant vigilance alone, but from environments where people can switch off, reset, and return with clarity rather than exhaustion.

Practically, the takeaway for MSPs is less about adding more processes and more about reinforcing the right behaviours around the processes that already exist. That includes building a culture where escalation is supported rather than penalised, where time off is genuinely respected rather than quietly discouraged, and where post-incident reviews focus on system improvements rather than individual fault. Webb's wider message is that resilience in cybersecurity does not come from constant vigilance alone, but from environments where people can switch off, reset, and return with clarity rather than exhaustion.

CHANNEL INSIGHTS 2026 ROUNDTABLE

MSP CHANNEL INSIGHTS ROUNDTABLE

Engage Directly with MSP Decision-Makers

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

SECURE YOUR 2026 PARTNERSHIP

VIRTUAL ROUNDTABLE

KEY BENEFITS:

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

EXCLUSIVE TO VIRTUAL:

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

CONTACT DETAILS:

Aadil Shah
aadil.shah@angelbc.com

SCAN ME

AUDIENCE INCLUDES MSPS, MSSPS, VARS AND IT RESLLERS

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

msp-channel.com/roundtables

Scaling without sacrifice at Chorus: “Anyone can grow quickly if they’re willing to compromise on service quality. We’re not.”

Based on an exclusive interview with Nicola Saner, CEO of Chorus, this article takes a behind-the-scenes look at how the MSP is scaling in a fast-changing market, and the thinking behind its approach to growth, service delivery, and long-term customer relationships.

CHORUS is a UK-based Managed Services Provider (MSP) and Managed Security Services Provider (MSSP) working with organisations that need their IT environments to be secure, resilient, and up to date without unnecessary complexity.

At the centre of the company is Nicola Saner, CEO. Her role covers setting strategic direction, building and supporting the leadership team, and making sure internal processes do not slow down delivery. Saner describes the company’s core direction clearly: “The core purpose hasn’t really changed: make technology simpler, safer and more useful for the people relying on it. That sounds straightforward, but in a market that moves this quickly it’s harder than it looks.”

That purpose has stayed consistent even as the MSP and MSSP landscape has continued to change. New security threats, evolving cloud platforms, and increasing operational demands have all added pressure on providers and their customers. Chorus focuses on identifying what genuinely creates value for customers and stripping out unnecessary complexity in how services are delivered.

How convergence is reshaping Chorus’s approach to growth

Chorus’s evolution has been shaped by a simple shift in what customers expect from their technology partners. As connectivity, unified communications, cloud, and managed IT services have converged, the demand for fragmented, single-purpose providers has steadily declined.

Saner describes this change as a turning point in the company’s development. “We’ve grown up, frankly,” she explains. Chorus began as a provider of strong point solutions, but the market moved in a different direction. Customers, she says, “don’t want twelve good vendors, they want one partner who joins everything together.”

That expectation has directly influenced how the business is structured today. Security, cloud, and managed services have been brought together into a single, more coherent offer, designed to reduce complexity and improve outcomes. The growth strategy that

follows from this is less about expansion for its own sake and more about alignment, with a focus on simplification and resilience.

This approach also extends beyond Chorus's direct customer base. Through its Cyber Channel Programme, the company works with other MSPs and resellers, providing access to enterprise-grade cyber capability that many would struggle to build internally. It reflects a broader intent behind the strategy, which Saner summarises as a mission to use technology to put people first, whether they are end customers or partners in the channel.

Scaling without compromising service quality

For Chorus, growth is not measured purely by speed. It is defined by whether the business can expand without weakening the standards customers depend on, or the conditions that allow teams to do their best work.

Saner is clear about the trade-offs many MSPs face. "Anyone can grow quickly if they're willing to compromise on service quality. We're not." For her, the priority is consistency at scale: "Fast and sustainable means scaling capability and capacity without burning out the people who make Chorus what it is."

The approach behind that balance is intentionally practical rather than flashy. "The balance comes from some fairly unglamorous things: governance, proper leadership layers, and discipline around where we invest." It is a model built on structure and restraint, ensuring that growth does not outpace the organisation's ability to deliver.

Shifting customer priorities across security and AI

Across the MSP landscape, Chorus is seeing a change in what customers expect from their providers. Saner points to cybersecurity and continuity as the most immediate pressure points. "Security, resilience and business continuity have moved firmly to the top of the agenda." That shift is also a key reason behind the launch of Chorus's Cyber Channel Programme, which is designed to help other MSPs access capability that is increasingly difficult to build internally. As she explains, "Demand for serious cyber expertise is outpacing supply right across the

industry, and other MSPs need a credible way to meet that need without standing up a SOC from scratch."

Alongside security, AI is becoming a more structured and less speculative part of customer conversations. Saner notes a change in tone rather than just interest. "On AI, the conversations have improved. Less hype, more focus on practical, safe use cases." She adds that customers are now more informed and more demanding in their questions than even a year ago, describing this shift as "healthy" for the direction of the industry.

That evolution is also shaping how Chorus is adapting its own services. Rather than treating AI and automation as standalone initiatives, the company is embedding them directly into its delivery model. The focus is on improving speed, insight, and operational efficiency, while keeping human expertise central to decision-making. She states that the intent is not to add technology for its own sake, but to make work more effective for teams and outcomes clearer for customers, whether they engage directly or through channel partners.

Knowing when to build and when to partner

As the MSP market becomes increasingly competitive and fragmented, Chorus takes a deliberately structured approach to deciding what to build in-house and what to source through partners.

For Saner, the starting point is clarity about value. "The test is fairly simple: if it differentiates us or directly shapes the customer experience, we build and own it. If it doesn't, we partner with specialists who already do it brilliantly." That distinction helps the business avoid spreading itself too thin, while still maintaining control over the areas that matter most to its customers.

Saner is direct about the risk of overextension in a crowded market. There is little value in duplication for its own sake, as attempting to cover everything typically leads to weaker outcomes rather than stronger ones. In her view, focus and selectivity are what ultimately protect both quality and relevance as the market continues to evolve.

What enables Chorus to scale without losing its edge

Chorus's growth has not been driven by a single breakthrough moment, but by a set of deliberate choices about how the business is built and run day-to-day.

Saner distils those foundations into three priorities: "Clear values, operational discipline, and a focus on customer experience." Alongside that, she points to an early decision that has shaped how the company scales in practice, investing in leadership and capability ahead of demand, rather than reacting once pressure builds. As she puts it, the aim was to avoid simply "bolting it on once cracks started showing."

That discipline matters because growth in an MSP environment quickly exposes inconsistency if it is not actively

managed. For Saner, the real test of scaling is not winning new business, but maintaining a consistent experience as the organisation expands. “The hundredth customer should get the same experience as the first,” she explains. In reality, that becomes harder with every new hire, every new service line, and every layer of growth added to the business.

Keeping that standard in place depends on more than process alone. It requires clear and repeatable ways of working, but also restraint in how much is standardised, applying structure where it genuinely improves outcomes rather than for its own sake. Alongside that sits a cultural expectation that quality is not optional, reinforced continuously rather than assumed.

As Chorus continues to scale, sustaining consistency ultimately comes down to culture. Described by Saner as collaborative and accountable, culture at Chorus is underpinned by a strong expectation of continuous improvement and trust between teams. Protecting it is intentional, starting with hiring decisions that prioritise attitude as much as skill, on the basis that behaviours are far harder to change than capability. That approach extends into how people are developed and supported as the company scales.

> The real question is how that technology is used in practice, under real operational pressure

The next phase for Chorus and the channel

Looking ahead, Chorus is less focused on short-term expansion and more interested in strengthening its role as a long-term partner for organisations that need secure and resilient digital operations.

Saner describes the ambition in simple terms: becoming the organisation customers rely on “when something matters.” That role extends into the wider channel as well, where Chorus is helping other MSPs build cyber capability at a time when demand continues to outpace supply.

It reflects a broader shift in the industry, where access to technology is no longer the main differentiator. The real question is how that technology is used in practice, under real operational pressure, and whether it genuinely improves outcomes for customers and partners.

Saner has a strong sense of the direction Chorus is taking and the foundations that will support it: “AI, cybersecurity and scalable operations are the engines that get us there. But the real differentiator won’t be the tech itself, because everyone has access to the same tools eventually. It’ll be how thoughtfully we apply it to help customers, and our partners, actually succeed.”

MANAGED SERVICES SUMMIT

BENELUX
LONDON
NORDICS
MANCHESTER

CREATING VALUE with MANAGED SERVICES

managedservicessummit.com

MANAGED SERVICES SUMMIT BENELUX

benelux.managedservicessummit.com

30 JUNE 2026

MANAGED SERVICES SUMMIT LONDON

london.managedservicessummit.com

09 SEPTEMBER 2026

MANAGED SERVICES SUMMIT NORDICS

nordics.managedservicessummit.com

05 NOVEMBER 2026

MANAGED SERVICES SUMMIT MANCHESTER

manchester.managedservices summit.com

17 NOVEMBER 2026

AI tools to digital employees: Why traditional security models are falling behind

Exploring how the rise of the digital workforce is reshaping cybersecurity. The discussion covers the shift from AI tools to "digital workers," why autonomous security models fall short, and how organisations must rethink governance, identity, and control by treating AI agents as employees within human–agent teams.

BY STEVE WILSON, CHIEF AI OFFICER AT EXABEAM

EXABEAM is a behaviour intelligence company for the agentic enterprise, aiming to deliver flexible, industry-proven solutions for insider threat coverage of humans and agents. Alongside this, Wilson also founded the OWASP GenAI Security Project, a global initiative of more than 25,000 contributors working to secure large language models and agentic AI systems.

In this interview, Wilson sets out a stark view of where enterprise technology is heading: away from traditional AI tools and towards a growing digital workforce of autonomous 'digital employees.' That shift is not just changing how work is done, but fundamentally reshaping the scale, speed, and nature of cyber risk. His perspective challenges assumptions around autonomous SOCs and human-in-the-loop models, instead pointing towards a future built on tightly governed human–agent collaboration.

These themes set the foundation for a wider discussion on why security, governance, and organisational design must evolve together if enterprises are to keep pace with the increase in data, agents and increasingly sophisticated threat activity he believes is coming.

The limitations of legacy SOC models

Wilson points to a fundamental mismatch between how security operations have evolved and the speed of today's threat landscape. While SOC tooling has advanced significantly over the past two decades, he argues that the underlying operating model has remained largely unchanged.

At the centre of the problem, Wilson says, is a model still built around human-led triage of overwhelming volumes of alerts. "The basic model is collect logs, have humans sort through the alerts, possibly giant piles of them, and try to make decisions fast enough to keep up with what's going on," he notes. But in today's environment, that approach is no longer sustainable, with the volume and speed of activity now outpacing what human-led processes can realistically handle.

What this means for MSP security strategies

Two major forces are reshaping the threat landscape and, in turn, changing what MSPs need to protect against. The first is the rise of what Wilson describes as the agentic enterprise, where organisations are rapidly deploying AI agents at scale. These are not simply chatbots, but autonomous systems capable of carrying out real tasks across business environments, bringing both productivity gains and new forms of risk.

Alongside this, threat actors are also adopting the same technologies.

AI-driven tools are increasingly being used to support offensive cyber activity, lowering the barrier for more sophisticated and scalable attacks. As a result, MSPs are no longer operating in a world where automation is purely defensive on the customer side.

The combined effect of these shifts is a significant expansion in both the digital workforce inside organisations and the volume of external threats targeting them. “You are going to be dealing with 100 times the amount of data, signal, and noise that your security operations team is going to have to sift through,” he explains. For MSPs, this creates a fundamentally different operating environment, where scale, complexity, and speed are all increasing at once.

Why autonomous SOCs fall short in an agentic enterprise

As the concept of an agentic enterprise gains momentum, Wilson draws a clear distinction between what AI agents are well suited for and where traditional security models begin to break down.

The starting point is understanding the fundamental strengths and limitations of both software and emerging AI systems. “Computers are good at maths. And they are good at repeatability,” he says, highlighting the strengths of traditional systems. In contrast, “AI agents, things built on large language models, they’re good at dealing with uncertainty, they’re good at dealing with unstructured data, and they’re great at dealing with language.”

The issue emerges when organisations attempt to replace traditional software with newer agentic models without fully recognising how fundamentally different their strengths and limitations are. This often results in using agents in contexts where they lack the consistency and judgement required, while still expecting them to perform highly structured and reliable tasks.

This mismatch is what ultimately undermines the idea of a fully autonomous SOC. The notion of handing cybersecurity entirely over to digital agents, without meaningful human judgement in the loop, is a direction he sees as increasingly unrealistic in practice. Instead of removing human judgement from the equation, he argues for a different model altogether. “We need to be building high-performance human agent teams, not autonomous SOCs.”

Rethinking the “human-in-the-loop” model

Wilson is quick to challenge the idea of a traditional “human-in-the-loop” approach, which he sees as an early and somewhat simplistic attempt to ensure oversight in AI-driven systems. In practice, he suggests, it often reduces human involvement to little more than repetitive approval tasks, with limited real impact on outcomes.

In many early implementations, humans are effectively reduced to validation roles, clicking through decisions generated by machines. Over time, this can lead to disengagement, where attention and accountability start to erode. In that scenario, the human becomes the weakest link rather than a meaningful layer of control.

The issue, he adds, is that this structure also undermines the very advantage organisations are trying to achieve with AI: speed. If every action requires human review, the system loses the efficiency gains that agents are meant to deliver.

Instead, he points towards a different model, where roles are more deliberately separated: human-on-the-loop. In this structure, AI agents handle high-speed processing of complex, unstructured data, while humans focus on judgement, context and accountability.

The goal is not to slow systems down with constant intervention, but to combine strengths more effectively. When designed properly, this balance creates high-performance human–agent teams, capable of managing the scale and complexity of an environment facing a dramatic increase in data and activity.

Where MSPs fit in the agentic security model

MSPs have traditionally been early adopters of new security technologies, and many are already beginning to integrate agentic capabilities into their environments. However, Wilson suggests the real opportunity lies not in replacing existing approaches, but in applying these tools to the parts of MSP operations that are still highly manual and costly.

One of the most immediate benefits is improving explainability. Earlier security models often generated large volumes of machine-led outputs that required significant human effort to interpret. In contrast, newer agent-driven systems

are better suited to translating complex security data into something more usable for human operators, particularly in environments where legacy systems still struggle to make findings intelligible at speed.

As Wilson argues, "we could have high-end models with thousands of rules that were processing the data being piped into your SIEM, your log aggregator, and it would pop out a finding that says, 'this is a problem'. Your humans then spend hours decoding that." He contrasts this with newer approaches that reduce that translation burden and make outputs far more consumable within the SOC.

Beyond internal operations, MSPs can also use these capabilities to extend communication with their customers, particularly in high-pressure situations where speed and clarity are critical. Agents can help streamline these workflows and improve how information flows during incidents.

At the same time, he cautions against viewing agentic systems as a simple replacement for existing automation. He points out that some capabilities are often misunderstood or overstated, particularly when applied to structured processes that still require deterministic reliability. "Go back to what are these things bad at? They're bad at maths. They're bad at repeatability," he notes, highlighting the risk of over-relying on agents in the wrong parts of the stack.

For MSPs, the value doesn't come from replacing what already works, but from integrating agents in the right places. The focus shifts to using them where they improve clarity and efficiency, while established systems are still relied on for consistency and reliability where it matters most.

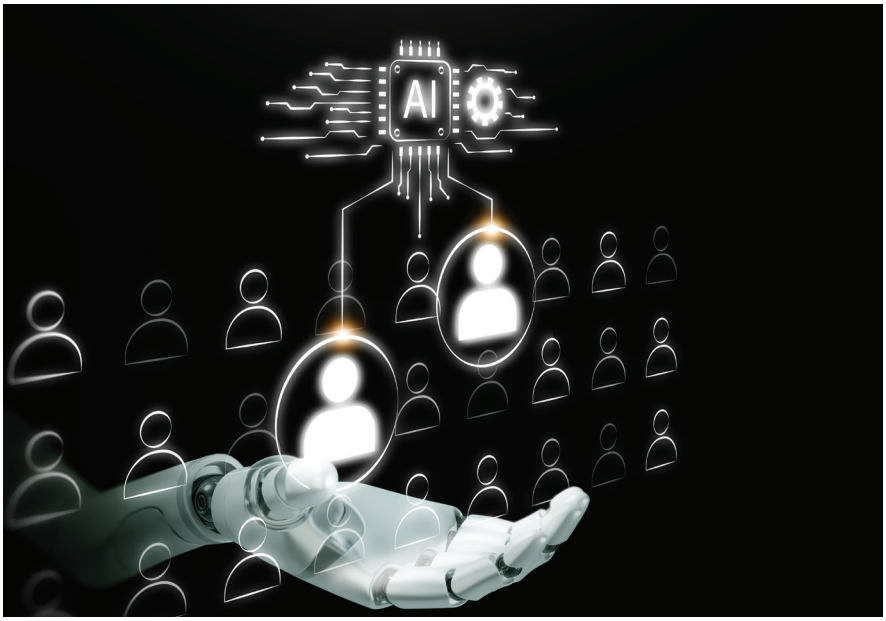
The digital workforce: when AI agents become employees

Wilson frames governance and accountability around a deeper shift in what these systems are becoming, and the extent to which existing language is already struggling to keep up. He notes that the term 'AI agent' has become so expansive that it has effectively lost precision, describing how it can simultaneously mean everything, and nothing at all.

That ambiguity, he suggests, reflects a change in the underlying architecture itself. Rather than short-lived, prompt-based tools, he describes systems designed for continuous operation and execution, explaining that "these are not prompt and response architectures. These have what are called 'agentic loops', they run 24 hours a day."

From this perspective, the shift is not just technical but structural. These systems are no longer episodic tools sitting inside workflows, but persistent entities that carry out work over time.

That is why he leans on the idea of 'digital workers' to describe them, and extends the comparison into organisational design itself. As he puts it, "I'm going to onboard them, I'm going to assign them an identity, I'm going to assign them access to the applications that they need, and only the applications that they need."



This framing fundamentally alters how accountability is applied. Instead of treating these systems as conventional software, he suggests they should be handled in the same way organisations think about human actors inside their environment, noting the need to "treat these as potential insider threats, just like I do my humans, rather than treating them as software applications."

MSPs in the age of digital workers

Looking ahead, Wilson places MSPs at the centre of an escalating security challenge shaped by both scale and speed. He highlights a sharp rise in AI-enabled activity, with threat environments becoming increasingly dense and difficult to manage as automated systems generate and process vast volumes of data.

In this context, the traditional MSP role is shifting. Once primarily focused on supporting organisations without in-house security capability, MSPs are now operating in an environment where even large enterprises are struggling to keep pace with the complexity of modern threats.

Wilson emphasises that the accessibility of advanced offensive tools is accelerating quickly, with capabilities emerging far closer to the frontier than many organisations are prepared for, and rapidly diffusing into the wider threat landscape.

Against this backdrop, he sees the opportunity for MSPs in adopting agentic technologies in a structured way, particularly by building hybrid models that combine human expertise with AI systems rather than pursuing full automation.

He also highlights a shift in security analytics, where organisations will need to monitor not just people, but the behaviour of autonomous agents operating inside their environments. For MSPs, this marks a clear opportunity to stand out by building capability in this emerging layer of visibility. Those that move early will be better placed to handle rising complexity and secure higher-value enterprise work.

CHANNEL INSIGHTS 2026 ROADSHOW

MSP CHANNEL INSIGHTS ROADSHOW

SECURE YOUR 2026 PARTNERSHIP

Taking the MSP Channel on the Road
2026 Regional Series

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

REGISTER NOW

Why Partner With This Series?

Pan-European Reach With Local Market Impact

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

Decision Makers in the Room

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

Curated Conversations That Convert

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

Beyond the Event

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

SCAN ME

msp-roadshow.com

Technician to leader: The art of letting go

In an exclusive podcast discussion, Craig Sharp, Owner and Founder of Abussi, shares his journey from hands-on IT technician to business leader, highlighting how growth requires letting go of day-to-day tasks and trusting others. He discusses how leadership focuses on communication, delegation, and strategy over technical skill.

Growing with the pace of the IT industry

SHARP TRACES his path in tech back to the earlier days of home computing, a time when enthusiasm for technology often clashed with scepticism about its future. He recalls working with ZX Spectrums and early tech in the 1980s, always knowing he wanted to work in the field, even if others weren't convinced it would last. His parents were sceptical about computing as a long-term career, so he initially explored more traditional options before eventually being drawn back into technology.

That return wasn't a straight line into engineering, but a shift in perspective. Rather than pure hands-on development, he re-entered the industry through project management, marking an early example of how his role would evolve alongside the sector itself. What followed was a business journey that began in 1995 with training and early software development using Microsoft Access, before gradually expanding into a value-added reseller model in the early 2000s. By around 2010, the company had again adapted, this time becoming an early adopter of the managed service provider model. This was a shift that reflected where the wider IT landscape was heading.

Today, Abussi remains deliberately lean but geographically distributed, with work spanning MSP management alongside software and workflow development. Sharp notes that this direction wasn't accidental but aligned with market momentum, describing how "the vast majority of our work now is higher-level MSP management, workflow and software development, because that's where the market is going."

His own role has transformed just as dramatically as the business itself. Where once he would be on-site, physically fixing issues and working directly with infrastructure, his day-to-day is now firmly rooted in leadership and oversight. Underlying this evolution is a mindset shaped by one influential idea from early in his career: Michael E. Gerber's E-Myth. The core lesson, he explains, is about structure and growth. When you start out, your name appears in almost every box, but leadership is about steadily removing yourself from those boxes and replacing your role with capable people who can own them. It reflects both his own progression and the wider shift in tech from hands-on technical work to systems delegation and leadership at scale.

Why letting go is the key to growth

Sharp describes delegation not as a management technique, but as a fundamental survival skill for any

growing business. One of the earliest and most important shifts he made was removing himself entirely from financial operations, a decision he still sees as pivotal. He explains: “The first thing that I did, which was the best thing I ever did, was move all financial management, day-to-day bookkeeping, anything to do with finance, to an external company,” adding that this external support became essential to stability.

That experience set the tone for how he thinks about responsibility more broadly. For Sharp, growth only happens when ownership is genuinely transferred, not just shared in theory. He is explicit about the core principle that followed: “I think the big lesson to learn is if you’re a business owner, you can’t hold onto it all, you have to delegate and give responsibility to other people.” It’s not framed as optional, but as a necessary condition for scale.

He also acknowledges that this is not a clean or instinctive transition. Moving from being the person who does and fixes everything to someone who trusts others to do it better is, in his experience, uncomfortable and ongoing. Even when a team is fully capable and the business is running smoothly, the instinct to re-enter decisions can remain strong. What changes over time is not just structure, but identity, shifting from being embedded in day-to-day execution to operating above it.

That evolution is what separates early-stage operators from long-term leaders.

That evolution is what separates early-stage operators from long-term leaders. The role stops being about controlling tasks and becomes about creating the conditions where others can take ownership and perform without constant intervention

The role stops being about controlling tasks and becomes about creating the conditions where others can take ownership and perform without constant intervention.

He also frames it as a question of perspective. Being in an industry for a long time can make it harder to see things clearly, as approaches evolve and people bring in newer skills, fresh thinking, and often better ways of doing things. At that point, strong leadership is about recognising you may not always be the best person for the job anymore, being willing to step back, and allowing others to lead where they are stronger.

Managing customer expectations and misconceptions

Sharp highlights that one of the most overlooked challenges in moving from a technical role into leadership lies not just internally, but in how customers and teams continue to perceive you.

In his experience, especially in a small-to-medium IT business that has grown over time, many long-standing clients still associate him with the hands-on technical work he once did. In his view, “the biggest problem that you have is the customer understanding that you’re not that guy anymore. Or you’re not that woman anymore. You are not the person to speak to about a day-to-day technical issue.”

Instead, the reality has shifted completely. He describes moving into a management role while former technical responsibilities are still associated with him by others in the business. That gap between how he is perceived and what he actually does has become one of the most persistent challenges in leadership.

The discipline is in deliberately stepping back and resisting the urge to get involved where it is no longer necessary. The real risk is that even a well-intentioned intervention can pull you straight back into the old perception of your role, undoing the shift you’ve made, and reinforcing the idea that you are still the person directly handling technical issues rather than the one leading the wider organisation.

Burnout and decision fatigue

Burnout and decision fatigue often come from trying to hold onto too much for too long, especially in leadership roles where the number of small daily decisions never really stops growing. The way through it starts with people rather than processes: “find good people in your business. Trust them, give them a clear framework of operation, and let them get on with it.”

Once the right people are in place, a lot of the pressure naturally begins to ease. Strong teams, he argues, don’t just take on tasks, they take on responsibility when properly trusted. But even then, the challenge is internal. A key part of reducing that mental load is letting go

of perfection as the standard. “Perfect is a relative activity,” he says, and chasing it can actually slow everything down. Instead, “good is acceptable, good is what most people want, good is fine. Perfect will get in the way of you providing good.” That shift alone removes a constant layer of pressure to step into every detail.

This can often mean being involved in only a fraction of a function, while the majority is handled elsewhere, allowing him to focus only on the more complex or high-stakes issues rather than the day-to-day noise. There will always be edge cases and problems that need senior input, but those should be the exception rather than the default. The goal is to avoid being pulled into everything, and instead focus energy where it genuinely adds value.

Building teams that understand people, not just tech

A big part of building the right team is realising that the best people are not always the ones with the most traditional technical backgrounds. In fact, some of the strongest hires can come from completely different industries. He points to two employees in particular at Abussi who came from customer service roles in a cinema.

What stood out, he explains, wasn’t their technical knowledge, but how well they translated skills like communication, patience, and empathy into a technical environment. Over time, they proved to be among the best people they had ever employed, because they grasped something fundamental about the industry: “it’s not about the tech. The tech is a secondary thing to what it is you’re trying to achieve for the customer.”

That shift in perspective reframes what good IT service actually means. It’s not just systems working, but outcomes for people. What customers really need is “reliability, safety, good advice, and for their IT systems each day to not metaphorically kick them in the head when they turn them on every morning.”

Because of that, he places huge value on interpersonal skills within his team. Being able to communicate clearly, listen properly, and avoid talking down to customers is just as important as technical ability. The goal is to have people who can empathise with a person’s problem rather than defaulting to technical jargon or superiority. The better outcome comes from keeping things simple, human, and honest, and treating it as a conversation rather than a demonstration of knowledge.

Ultimately, he argues that if customers already understood IT at a deep technical level, they wouldn’t need external support in the first place. The value of the service, therefore, lies not in showing how much you know, but in making things understandable and genuinely helpful.

Stepping back to move forward

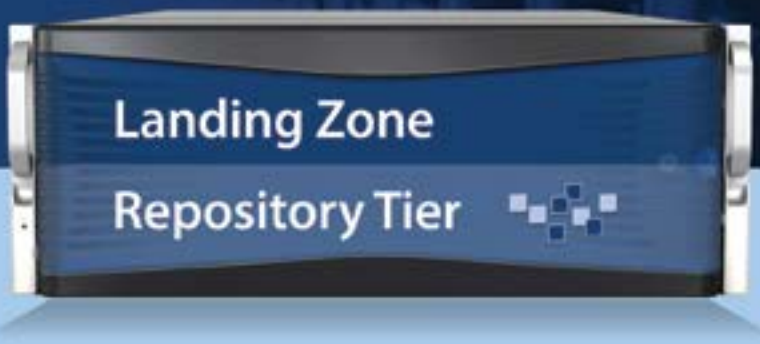
Overall, leadership in the IT channel isn’t what it used to be. It’s no longer about being the person who can fix everything, answer every question, or sit closest to the technical detail. For leaders like Sharp, the role moves away from day-to-day technical delivery and towards something far more difficult to define, and arguably harder to master.

It’s about translation. Between customers who don’t speak “tech” and engineers who live in it. Between what a business wants and what is actually possible. Between urgency, expectation, and reality. But it’s also about restraint. Knowing when not to get involved. Stepping back so others can step forward. Trusting people to do the work better than you do.

And underneath it all sits a consistent theme from Sharp’s experience: leadership is less about doing more, and more about doing less. Delegating properly. Building strong people around you. And accepting that success in the channel isn’t about holding everything together yourself, but making sure you no longer have to.

EXAGRID
Tiered Backup Storage

The future is here.
Tiered Backup Storage



FASTEST BACKUPS

FASTEST RESTORES

SCALABILITY FOR FIXED-LENGTH BACKUP WINDOW

COMPREHENSIVE SECURITY WITH RANSOMWARE RECOVERY

LOW COST UP FRONT AND OVER TIME

MSP CHANNEL AWARDS
2025 WINNER

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

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

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

LEARN MORE >

Guardz Q&A: Agentic AI, strategic partnerships and building MSP-first security platforms

In this Q&A, Doni Brass, SVP Product Strategy & Community at Guardz, discusses how MSPs are adapting to rising cyber threats, the shift toward platformisation, and how AI-driven automation and strategic partnerships are reshaping security delivery for small and medium-sized businesses.

Sophie Milburn: To begin, could you introduce yourself, your role at Guardz, and provide an overview of the company and its focus?

Doni Brass: I'm Doni Brass. I lead our product strategy and community at Guardz, and Guardz is a cybersecurity platform. We're specifically focused on MSPs, and the MSPs who are serving small to medium-sized businesses. The value of our platform is really our ability to bring that security to the backbone of our economy, the 99% of businesses that otherwise would not be secured, and that's what I'm here to talk about today.

Sophie Milburn: Guardz has grown significantly in recent years. What do you think has driven that growth, and what do you think is the strongest demand from MSPs today?

Doni Brass: Cybercriminals are scaling because of AI and attack-as-a-service models, which are reaching all-time highs. Small businesses historically had some security by obscurity, which allowed them to fly under the radar. But now even an amateur hacker can pay around $150 a month for an attack-as-a-service kit on the dark web. They can run a spray-and-pray campaign, spin up websites that look like any bank or social platform, steal credentials, and then either exploit a company directly or move through the supply chain.

The MSPs we work with want automation and outcomes. They are overwhelmed by tools and complex systems that were not built for them. By streamlining cybersecurity into a unified platform, Guardz brings the necessary tools together and automates the operations they struggle with. That is where we have seen the most growth, reducing complexity and improving execution.

Sophie Milburn: With that, I'm assuming that the expectations towards Guardz have changed a lot from both a customer and an MSP standpoint, so what do you think differentiates someone that adopts Guardz successfully and those who perhaps don't leverage its full potential?

Doni Brass: I would say the expectation shift is from siloed tools to platforms. Platformisation has been happening in the cybersecurity world at the enterprise level for the better part of a decade. But those tools are not built for MSPs. MSPs have either had to use very complex tools that are not designed for them, or they have gone toward point solutions, meaning more focused individual tools. Then they are left trying to operationalise everything.

The move to turn-key platforms, this platformisation approach, is now reaching the MSP market. That is where the expectation has shifted toward Guardz. But the MSPs who succeed are really the crux of the question. I would say it is the MSPs

who treat security as a core offering and embrace automation to achieve that.

The MSPs who struggle are still trying to piece fragmented tools together. That often requires more tooling, including SIEMs and SOARs, and other layers of complexity. Those tools also rely on an older way of approaching detection and response. AI is reshaping this. Autonomous workflows, or agentic workflows, are changing how people address security needs, and that is where things are really moving the needle.

Sophie Milburn: How would you say that your partnerships with companies like Check Point, SentinelOne and Pax8 translate into tangible value for MSPs, and how do you prioritise partnership strategy when trying to scale?

Doni Brass: Those partnerships, specifically the ones you mentioned, have allowed us to build trust with our client base. Bringing different tools together has been an important part of what we do, and we have our own IP to support that. Combining that with names like Check Point and SentinelOne also brings trust. For us, that has been a key go-to-market strategy.

Bringing best-in-class controls not only to our brand but also to our MDR experience is important. Our MDR is 24/7, with agentic triage and human-led response. That is a major part of how trust is built. Integrating best-of-breed brands into that stack also enables faster time to value.

We prioritise partnerships that integrate deeply into our platform and scale globally. With companies like Pax8, for example, we are doubling down on the relationship, not from a security perspective but from a distribution perspective. Their marketplace stands out, and we align closely on values in how we approach our client base.

Sophie Milburn: How would you say that AI is embedded within the platform, and what practical impact do you feel like it's having?

Doni Brass: My answer to this question has changed maybe three times in the last six months. We have had AI, what I would call generative AI, in the platform from day one. We are a four-year-old company, and we have always used it in ways like generating phishing emails, explaining threats to end users or MSPs, summarising data, and providing insights. That kind of generative AI has existed in the platform for a while.

What has changed more recently is the shift toward agentic AI, agentic workflows, and now more autonomous workflows. The most impactful use today is happening in the triage layer. There are many signals coming in, and because we are unifying different tools, we rely on a single data lake with normalised logs and detection data. We correlate those signals, but there are naturally many false positives. If you work from noisy data, you create more noise.

The agentic triage layer helps filter that noise. It passes enriched, clean data to human analysts, with clear reports and recommendations, allowing them to work more efficiently. That is happening on the backend and in the MDR side of things.

What we are starting to do now, and this is the most exciting part, is bringing autonomous analyst capabilities into the platform itself. MSPs will be able to interact not only with generative AI in a reactive way, but proactively with agentic tools. They will be able to say, here is how we can improve security, here is how we can reduce response time, and the AI will present recommendations directly to admins.

Instead of handing things only to Guardz analysts, it will hand them to MSP admins and say, here is what we recommend, and in some cases, I can do this autonomously if you approve it. That trust will be built over time through workflows, and it will solve more problems

We have had AI, what I would call generative AI, in the platform from day one. We are a four-year-old company, and we have always used it in ways like generating phishing emails, explaining threats to end users or MSPs, summarising data, and providing insights.

in a much shorter period of time. The human in the loop is still an essential part of this. We're not looking at the autonomous analyst to replace the human. It's about supplementing the skill set of the MSPs and of their teams and technicians.

Sophie Milburn: What do you think sets Guardz apart from other cybersecurity platforms?

Doni Brass: Guardz was born in the age of AI, which is a major advantage. If you think of companies that have existed for decades and have built large "aircraft carrier" organisations that have moved in a certain direction, they may be excellent at what they do, but steering that ship is not easy. Adapting to this new world is not easy. We were built to be truly AI-native from the beginning, which gives us a significant advantage.

I would highlight three things.

First is our approach to security. We unify best-of-breed tools and connect the dots across them. When we detect different signals, we can piece together what is happening in the attack chain and stop attacks as early as possible. From a security perspective, this is something we do very well and where we stand out.

Second is our focus on operational efficiency. Security is only as strong as an MSP's ability to operationalise it, and Guardz gives them the tools to do that. Enterprise tools are not always built for MSPs. Even with the best tools, if you cannot operationalise them or

We recognise that MSPs are also small and medium-sized businesses with needs beyond security and IT. They need to grow their business, market themselves, communicate value to clients, and retain those clients. We have built tools for prospecting new business, conducting security business reviews to demonstrate ongoing value

turn them into an effective, manageable security programme, they are less effective. We simplify security in the way MSPs work, and that is a major part of what we do.

Third, we recognise that MSPs are also small and medium-sized businesses with needs beyond security and IT. They need to grow their business, market themselves, communicate value to clients, and retain those clients. We have built tools for prospecting new business, conducting security business reviews to demonstrate ongoing value, and a partner portal and programme where MSPs can get certified and access materials to run campaigns across social and email. All of this is designed to support them as businesses that need to grow, scale, and communicate their value.

These are the key factors that help us stand out.

Sophie Milburn: Looking ahead, what do you see evolving within the platform, and what are you looking forward to for MSPs in the next couple of years?

Doni Brass: I think automation is really the key. MSPs need to evolve in a way where they can support more clients per technician, and increasingly that will be driven by automation and agentic AI. That is just the math that has to happen financially speaking.

They have already become by default security providers. The MSP was not born as a security provider. It started in the IT space and has grown into becoming security providers.

The line between MSPs versus MSSPs has gotten fuzzy, although there are still distinct differences.

I think Guardz will be the foundation for enabling the shift toward automation and toward building security into the core offering of many MSPs. The partners we are working with who are the most successful are really steering that ship as well, and we are proud to be a part of it.

CHANNEL INSIGHTS 2026 ROADSHOW

MSP CHANNEL INSIGHTS ROADSHOW

SECURE YOUR 2026 PARTNERSHIP

Taking the MSP Channel on the Road
2026 Regional Series

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

REGISTER NOW

Why Partner With This Series?

Pan-European Reach With Local Market Impact

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

Decision Makers in the Room

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

Curated Conversations That Convert

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

Beyond the Event

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

SCAN ME

msp-roadshow.com

DigiCert Q&A: AI threats, certificate lifecycle risk and channel strategy

In this Q&A, Christian Stanford, RVP EMEA Channels at DigiCert, discusses the company's channel-first strategy, the growing urgency around certificate lifecycle management, and how partners can help organisations navigate AI-driven security risks, compliance demands and emerging threats such as quantum computing.

Sophie Milburn: Could you introduce yourself, your role at DigiCert, and give us a brief overview of the company and what it focuses on?

Christian Stanford: My name's Christian Stanford. I'm the Regional Vice President of EMEA Channels at DigiCert. I've been tasked with running the channel team for EMEA and I'm responsible for the regional strategy. While we've more recently expanded our focus in the channel, we bring a long-established customer base and strong enterprise heritage. That creates a significant opportunity for partners, who can tap into existing demand while building new business through a collaborative, give-to-get approach.

DigiCert is trusted by thousands of customers globally to deliver intelligent trust, through our comprehensive platform called DigiCert ONE. Our platform brings together PKI, DNS and certificate lifecycle management in one place. It enables organisations to enforce policy, secure AI-driven systems and prevent outages, while managing certificates and trust at scale. The platform is where we are seeing the most partner interest today, bringing together TLS and DNS technologies, while enabling the management of everything DigiCert offers through a single interface.

Sophie Milburn: Deepfakes, identity-based attacks, and AI-driven exploits are on the rise. What should organisations prioritise to try and safeguard their data and maintain operational resilience today?

Christian Stanford: It is increasingly difficult to tell what is real from what is fake these days. One of the most important priorities is being able to prove where content comes from and whether it has been altered. That is the focus of our new AI technology called Content Trust Manager, which enables organisations to sign and verify digital media at scale. By cryptographically signing content, it embeds trust into the content at the outset and means organisations can give users confidence in what they are seeing to help protect their brand from manipulation and misuse.

Another key challenge for enterprises is the continued shortening of certificate lifecycles. Following industry changes, the maximum validity period for TLS certificates is being reduced to 200 days from March 2026, with further reductions expected to 47 days by 2029. This means organisations will need to renew and manage certificates far more frequently than before. Many still lack visibility into how many certificates they have, where they are deployed and when they expire, creating real operational and security risk. As lifecycles shrink, automation and centralised management become essential to maintain resilience and avoid outages at scale.

Sophie Milburn: DigiCert operates across a wide range of highly regulated industries globally. How can partners help clients navigate complex compliance requirements while also implementing effective security practices?

Christian Stanford: It's first worth pointing out that DigiCert is trusted by the majority of the Fortune 500. DigiCert customers span multiple verticals. It won't be a surprise to many, but they include finance, healthcare and retail, as well as the public sector, government, manufacturing and defence, which is obviously very important given what's happening in the world today.

Manufacturing is particularly interesting for partners right now because DigiCert is quite different to others in that it enables the protection of IoT devices. This means we can support IoT environments across sectors like automotive and industrial. All of this can be managed through the DigiCert ONE platform, which can handle certificates and devices at vast scale. This is built for the enterprise and the mid-market as well.

Partners can provide services powered by our platform, and many are already doing so. In turn, they are helping their clients stay compliant around PKI and identity, which is very much a priority, while also being in line with industry standards. We align with most major frameworks, but to name a few, NIS2 and, of course, GDPR. The key point is that partners are able to simplify compliance adoption and help maintain those standards on behalf of their end clients.

Sophie Milburn: How is DigiCert working with partners through its channel programme, and what value does the ecosystem provide to MSPs, MSSPs and systems integrators?

Christian Stanford: One thing I haven't mentioned so far is that we have a full and comprehensive partner programme. The programme is built for technology partners, technology integrators, systems integrators, GSIs and, of course, MSPs, MSSPs and resellers. Our partnership programme covers all the bases.

DigiCert is expanding its channel presence and adopting more of a channel-first approach in some areas. This means we don't just offer a programme with all the trimmings. We also provide education and enablement tools, essentially everything a partner would need. We maintain strong margins, which is very important for partners. We also provide tiering based on investment, along with badges and certifications.

I would point out the most important thing for partners to hear is that our sales team is fully aligned with the partner ecosystem, and we work very closely across DigiCert sales, partner sales and end clients. As I mentioned, we have a give-to-get approach, where we have a large base of customers that we can introduce to partners, and in return, partners can introduce us to some of their customers.

Sophie Milburn: What practical steps can MSPs take to build trust and credibility in digital resilience and identity management?

Christian Stanford: For MSPs, GSIs and resellers, building trust and credibility in digital resilience and identity management starts with delivering consistent, scalable services that customers can rely on. That means moving beyond simply reselling certificates, and instead offering managed services around PKI, DNS and certificate lifecycle management.

We are seeing strong demand from partners for platforms that allow them to do exactly that. DigiCert provides a unified platform that enables partners to manage certificates, automate lifecycles and enforce policy at scale, giving them the foundation to build repeatable, high value services for their customers. Capabilities such as trusted lifecycle management allow partners to improve visibility, reduce risk and help prevent outages.

Alongside that, our partner programme is designed to support partners as they build out these services, providing the enablement, tools and access they need to develop skills, differentiate their offering and deliver trusted outcomes for customers.

Sophie Milburn: How does DigiCert's partner ecosystem support organisations in delivering secure and scalable solutions? And what advice would you give to those looking to optimise the use of that programme?

Christian Stanford: End clients are managing thousands of certificates in

some instances, sometimes less, sometimes more. But this is really the lifecycle of certificate question, and it is shortening. Customers of partners don't have these comprehensive plans in place. That's what we're hearing, that's what we're finding and that's what partners are saying to me. This makes it difficult to manage the volume of certificates that some clients have in place, as well as the shorter lifecycle requirements. Automating these often repetitive and manual processes is crucial.

Sophie Milburn: What are you excited about in the next couple of years, and what emerging technologies, threats and trends do you anticipate having the biggest impact in the years to come?

Christian Stanford: MSPs need more help than ever because of the shortening lifecycle of certificates of their customers and the mandate that has been put in place. It has crept up on people. The renewal cycle is 200 days as of this month, reducing to 47 days by 2029. So, organisations are looking to reduce cost, risk and achieve compliance by shifting towards automation and AI.

Secondly, what we are hearing, and this did come out of RSA, is it's obvious everyone is talking about AI, but the trending topic is the threat of AI. Getting ahead of that and the looming challenge of quantum computing. Google recently projected Q-Day to be sometime in 2029 and we are uniquely positioned to support enterprises as they look to become quantum-ready, and safe. Partners are crucial in this regard because it requires preparation to start now if it hasn't already, and the shared expertise is what will enable organisations to get ahead.

How channel partners are managing overconfidence in AI controls

As AI adoption accelerates, many organisations are discovering a growing gap between visibility and control. For MSPs and MSSPs, helping customers manage AI risk is emerging as both a security challenge and a strategic opportunity.

BY RYAN DAVIS, CHANNEL ACCOUNT MANAGER AT CULTUREAI

AS ARTIFICIAL INTELLIGENCE becomes progressively embedded across business operations, a new risk has emerged. This risk comes not from a lack of adoption, but from misplaced confidence when it comes to visibility. Recent research reveals that while 72% of organisations think they have full visibility into AI use, 65% continue to uncover shadow or unauthorised activity. This stark disconnect highlights a growing 'AI control gap' that is quickly becoming one of the most pressing challenges in enterprise security. Most businesses, especially those in highly regulated sectors, acknowledge the risk, but don't understand the breadth or know how to control it properly.

With the right context, channel partners can help customers navigate a rapidly widening gap between AI adoption and control. So what do MSPs and MSSPs actually need to understand about this shift, and where's the real opportunity to lead?

Navigating the gap: understanding where it comes from

At the centre of this issue is a fundamental misunderstanding of how AI tools are actually being used day to day. Employees are increasingly turning to generative AI platforms to boost productivity, often without formal approval or oversight. These tools are easy to access, difficult to track, and frequently operate outside traditional security perimeters. As a result, sensitive data is being exposed, compliance requirements are being breached, and many organisations do not even realise it is happening.

What's become clear is that banning AI usage altogether will not work, especially when employees are already seeing value from these tools. In the case of a full ban, employees may resort to using generative AI on personal devices, outside any form of visibility or control. This creates even greater risk and removes any chance of intervention.

This is where channel partners, particularly MSPs and MSSPs, step into a critical role. As trusted advisors, they are well-positioned to help organisations navigate the complexity of AI adoption while addressing the risks that come with it. For partners, the

widening AI control gap presents both a technical challenge and a strategic opportunity. So how can channel professionals best support customers in this space?

The opportunity: empowering AI users, securely

For many partners, the first step is helping customers understand that visibility does not equal control. Many organisations, more than 60 percent according to research, already have frameworks, policies, and oversight in place. This is progress, but policy alone, or basic monitoring tools, is no longer enough.

AI usage is fragmented across teams, devices, and applications, making it difficult to build a complete picture. Governance exists, but behaviour sits outside of it. Channel professionals need to guide organisations toward a more realistic understanding of risk, one that accounts for both sanctioned and unsanctioned AI usage.

This shift creates a significant opportunity. AI is not just another security concern. It is a new category of risk that intersects with productivity, data governance, and human behaviour. Partners who can turn that complexity into clear, actionable insight will stand out.

In conversations with customers, the demand is consistent. They want practical guidance. What tools should be allowed? How should data be handled? How can employees use AI safely without slowing the business down?

From a commercial perspective, this opens the door to new services and revenue streams. Advisory-led engagements around AI governance, risk assessments, and policy development are becoming more valuable. There is also growing demand for continuous monitoring and behavioural analysis to detect risky usage in real time. AI usage control is not a one-off project. It is an ongoing service model, and it plays directly to the strengths of MSPs and MSSPs.

What proper AI usage control looks like and why it matters

Effective support requires more than technical solutions. Proper AI usage control needs to balance security with usability. Overly restrictive policies push employees toward shadow tools, increasing the very risks organisations are trying to reduce.

Instead, controls should focus on visibility, education, and context.

This means understanding how AI is used across the organisation, identifying high-risk behaviours, and guiding employees in real time. It also means building a culture of responsible AI use, where people understand not just the rules, but why those rules exist. Channel partners have a key role to play here, helping organisations embed safe AI usage into everyday workflows rather than treating it as an afterthought.

Ultimately, the AI control gap is not a failure of technology. It is a reflection of how quickly adoption has outpaced governance. Businesses want the benefits of AI, but many are moving without the guardrails to do it safely.

As this gap continues to widen, the role of channel partners becomes more important. Those who combine technical depth with strategic insight will lead, helping customers move from guesswork to control, and turning AI from an unmanaged risk into a managed advantage.

Cognitive enterprises, autonomous firms, platformisation, and trust as a service are poised to shape the future of work

AI is reshaping work and business models, but future success will depend on how organisations harness human knowledge.

BY LAURA WENZEL, GLOBAL MARKETING AND INSIGHTS DIRECTOR, IMANAGE

WHEN PROFESSIONALS across a variety of different industries look into the proverbial crystal ball, they reach a similar conclusion: the nature of work will change in the next 10 years.

According to recent global research, global leaders overwhelmingly believe that AI-powered scenarios such as cognitive enterprises, platformisation, autonomous firms, and trust as a service will become a reality within the next decade.

Most expect these scenarios to have transformational impact on their organisations – but it's worth taking a closer look at the data to better understand what that change might look like, which organisations are most optimistic about the coming change, and what it will take to succeed in this next era of work.

The evolution that lies ahead

First things first: what do these terms – cognitive enterprises, platformisation, autonomous firms, and trust as a service – actually mean?

Fortunately, the survey of 3,000+ professionals that forms the basis of the global research report provided a specific definition for each one, to ensure that respondents were on the same page.

Cognitive enterprises are defined as a scenario where firms evolve to leverage AI to simulate legal, regulatory, and business outcomes as a service – essentially being paid to provide predictions.

Autonomous firms were defined as a scenario where AI agents conduct the standardised or repeatable document work (think: creating an NDA or a lease agreement) while professionals focus on strategic oversight and ethics.

Platformisation is a scenario where traditional professional services firms are replaced by digital platforms offering modular, on-demand business and consulting services where professionals work as independent experts.

Finally, trust as a service was defined as professional services firms offering trust services as a business – basically, being paid to verify what's "real" and what isn't, given the volume of deepfakes and misinformation from AI-generated content.

Different maturity levels, strikingly different outlooks

Here's where things get interesting. The study classified respondents by placing them along a knowledge maturity curve, from least mature to most mature.

All respondents, regardless of maturity level, were consistent in their response that these four scenarios were likely in the next 10 years. Where they diverged – greatly – was on whether these emergent scenarios would have a positive impact on their business or not.

Among the most mature enterprises, 88% to 92% felt that the impact of these scenarios on their business would be positive. Among the least mature, that number sinks to a notably lower range of 55% to 65%. That gap reflects two fundamentally different outlooks on the future of work.

Maturity breeds confidence

What accounts for this huge gap, where nearly twice as many members of one group are excited and optimistic about the unfolding of these four scenarios and the impact they will have?

The most mature organisations are focused on the quality of their data. They've made ongoing investments to establish a core knowledge foundation that newer technologies like AI can be layered on top of. This extends to people and processes: they have an approach to their human intelligence that captures it and ensures that it can be accessed to support key business goals and objectives.

Additionally, there is an openness to technology and change that is woven into the business culture of more mature organisations. In lessmature organisations, end users tend to resist new tools – only about 40% eventually embrace them, according to the research – whereas users in more mature organisations often adopt technology even before it's formally rolled out.

Together, these aspects make the most mature organisations confident that scenarios such as cognitive enterprises, platformisation, autonomous firms, and trust as a service will have a positive impact on their business.

A look at the future of work

With that foundation in mind, it becomes easier to examine how these scenarios are poised to transform work.

Start with the cognitive enterprise scenario, which is largely around predictive capabilities. AI can help model different scenarios and outcomes in ways that the human brain simply cannot. However, AI still requires human judgment and/or intelligence as its source material to deliver value – favouring the more mature firms that have processes in place to effectively capture it. This same human judgment will likely still play a role in validating outputs – the predictions actually provided to clients – underscoring the importance of the "human in the loop".

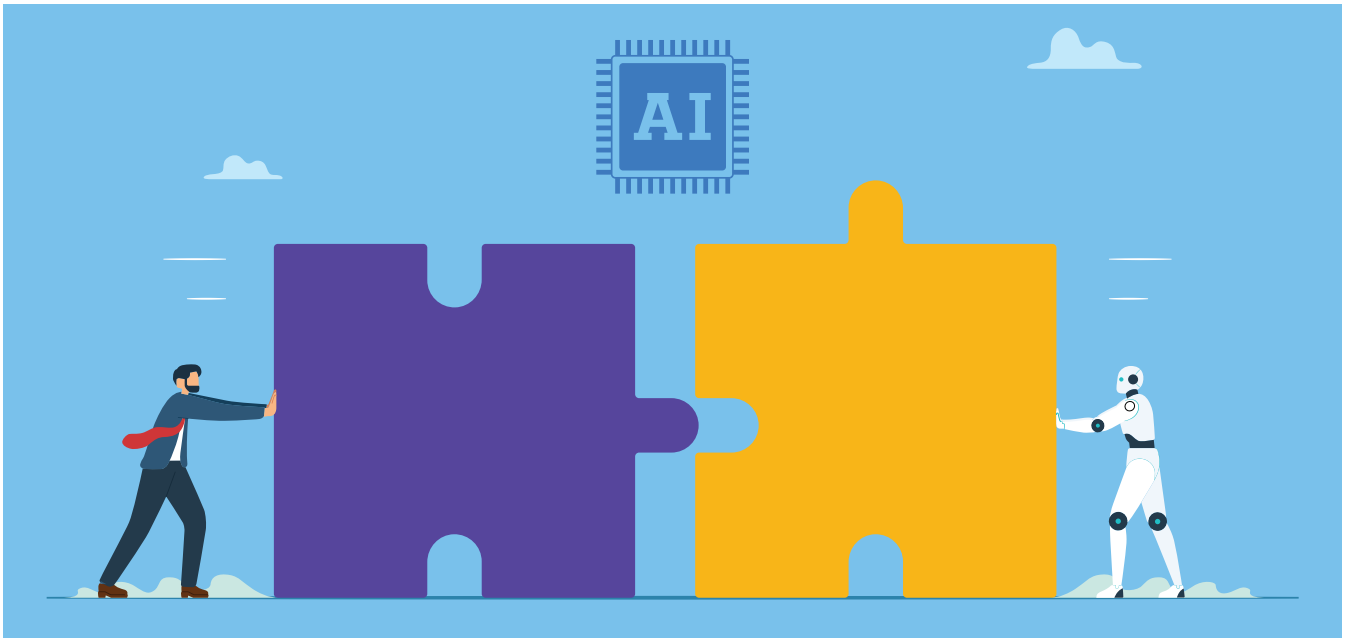
The autonomous firms scenario – which incorporates agentic workflows – extends this idea further by requiring not just a core knowledge foundation but also a precise understanding of their own workflows and processes. Without a clear map of how work actually moves through the organisation, there is no foundation on which to design or automate agentic behaviour.

In the platformisation scenario, it's easy to imagine enterprises shifting away from commoditised work products – like a standard legal form or relatively uncomplicated financial agreement – and delivering them through a consumption model, much like SaaS companies do today. At the same time, they can continue to offer higher value expertise and guidance services that help them maintain their profit margins. Again, none of this is possible without the initial investment in building a knowledge foundation, which mature organisations have undertaken.

Finally, there's the trust as a service scenario. While this might not be a standalone business offering, it seems likely that this will become another foundation that is required in order to produce a reliable service offering. So, there will be the data foundation, the governance layer, the AI infrastructure layer – and now, a trust layer.

The bottom line? AI is going to enable some exciting scenarios to come to pass, but not all enterprises are equally positioned to embrace these new business models and service offerings.

Even if AI has the power to help organisations deliver these new services at scale, there's still a fundamental dependence on human intelligence, judgment, and knowledge. The organisations that systematically capture and apply their institutional knowledge will be the ones most capable of transforming their business and adapting to the future of work that will take shape over the coming decade.



The hidden barrier to scaling a SOC: consistency, not technology

As MSSPs scale, maintaining consistent investigative quality becomes increasingly difficult. In complex SOC environments, long-term success depends not just on tools and automation, but on embedding context, judgment and trust into day-to-day operations.

BY DAN BRIDGES, TECHNICAL DIRECTOR, DROPZONE AI

AS MSSPs grow, scaling is often viewed as a sign that the organisation is maturing. More customers, more analysts and more tooling typically signal progress. Yet growth brings its own set of challenges, and one of the most persistent is the gradual loss of consistency in the service they deliver.

As SOC operations extend across shifts, geographies and increasingly varied customer environments, the method for conducting investigations can begin to diverge. These differences are often subtle at first, only becoming visible when trust or performance is being questioned.

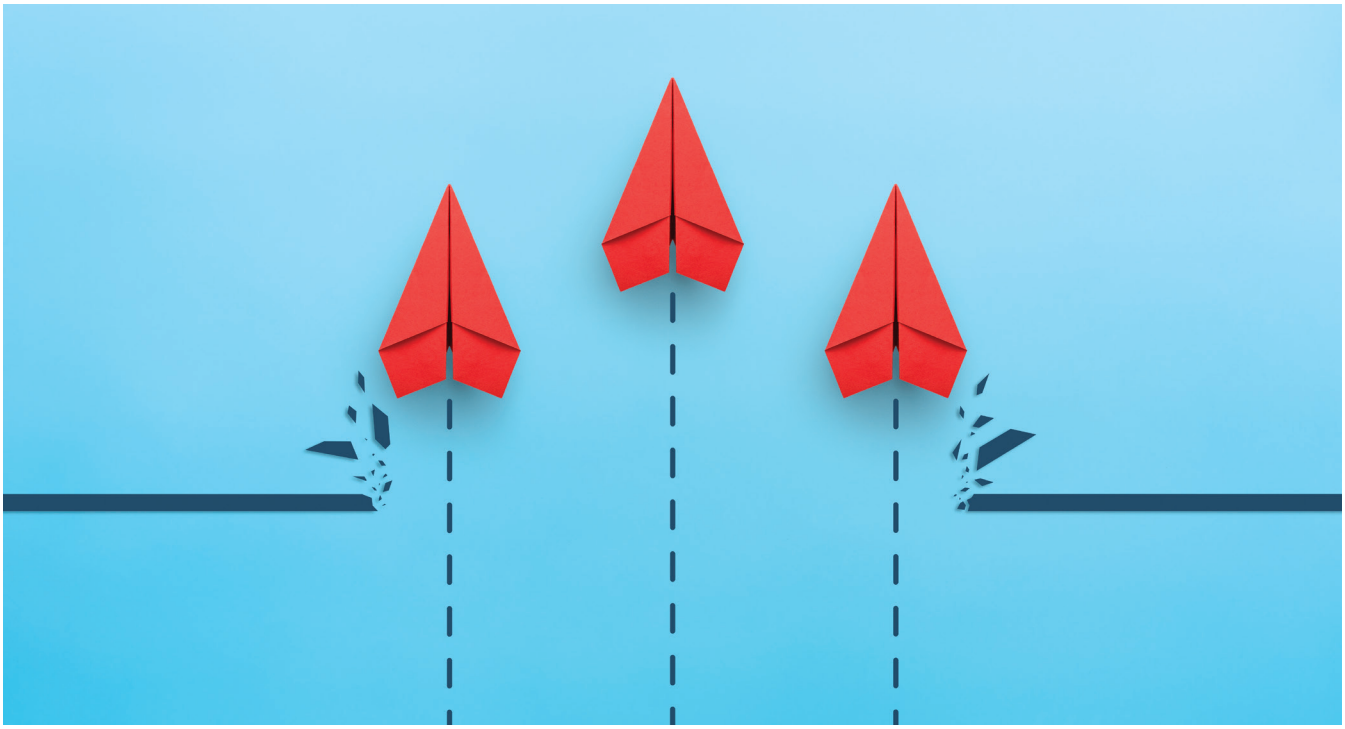
The human factor behind SOC inconsistency

Drawing on years of experience working within and alongside MSSPs, I've come to see consistency as the single hardest capability to maintain. Technology will scale as needed, but human judgment does not follow that same trajectory. When investigations depend on interpretation and experience, small variations quickly compound.

This becomes most apparent in situations that appear routine. For example, three analysts can start with the same alert and the same process yet reach different conclusions. None are wrong in their approach; their decisions merely reflect different investigation paths, different instincts or different weighing placed on certain pieces of evidence. However, from the client's perspective, the variation feels unpredictable. When outcomes depend on who is on shift at any given time, inconsistency shifts from an isolated occurrence to an operational concern.

The limits of automation and the real onboarding challenge

Automation can deliver a level of uniformity, particularly for familiar



patterns and routine tasks. But meaningful investigations require more than rule-following. Analysts must recognise nuance, interpret intent and understand the business impact of what they are seeing. As threats evolve and environments become more complex, the limitations of rigid automation become clear.

This is why the onboarding phase often highlights the challenges that are rarely a result of the technology. The real difficulty lies in understanding how an organisation functions, by learning its critical processes, essential systems and decision flows.

Analysts can interpret logs and alerts, but without understanding the operational context behind them, even accurate assessments risk missing the broader business impact. For MSSPs working across multiple industries, asking analysts to internalise every customer's operational reality simply does not realistically scale.

The critical role of context in understanding risk

The task becomes harder still when customers rely on bespoke internal systems. These often provide essential context for interpreting alerts, yet analysts may only see fragmented data.

At the same time, expectations around transparency and value have evolved. Clients want clarity on how decisions are made, how incidents are interpreted and how value is being delivered – particularly at the C-suite level. Ironically, when a SOC runs smoothly with no major incidents, the value becomes more difficult to articulate.

Fundamentally, strong investigative work depends on context. Two identical alerts can carry very different levels of risk depending on the systems involved. Quality is shaped by depth, clarity and reasoning, not simply the speed at which tickets are closed. In some cases, taking more time is the right decision if it leads to a more informed and confident outcome.

Why trust depends on consistency beyond the tools

Trust is shaped in the same way. Many customers are more comfortable with a false positive than a missed threat,

especially early in the relationship. Clear reasoning and transparent communication build confidence, while inconsistency erodes it quickly.

This is also where the limits of traditional automation become apparent. Tools can enforce process, but they cannot replace sound judgment or interpret ambiguous signals.

Another challenge lies in the way context is retained. Even with strong procedures, analysts work across multiple customers, and remembering which rules apply where is difficult. Pod-based models create familiarity, but they also create dependencies and when experienced team members leave, critical knowledge often leaves with them.

The future of SOC operations depends on making this knowledge transferable and embedded in systems rather than reliant on individuals.

There is also a noticeable gap between how SOC services are purchased and how they deliver value. Procurement focuses on tooling, SLAs and coverage, factors that are easy to compare on paper. Yet the most meaningful differentiator is the quality and consistency of day-to-day investigative work, which is much harder to quantify. Scale may increase capacity, but it does not guarantee better outcomes. In many cases, it amplifies inconsistencies already present.

Why consistency must become a strategic priority

As MSSPs look ahead, priorities need to shift. Speed alone will not resolve the most complex challenges. Analysts work under constant pressure, knowing they must be accurate every time while attackers only need to be successful once. Scaling a SOC should not be about removing people from the process, but about ensuring that human judgment is applied consistently and supported effectively.

Ultimately, consistency is what gives customers confidence in their security operations. It is also the capability most affected by growth. The vendors that succeed in the near future will be those that treat consistency as a discipline, one built on clarity, context and the ability to make human judgment as dependable as the systems designed to support it.

Why digital transformation strategies fail in delivery - not design

Why do so many transformation programmes lose momentum after a strong start? Sustained success depends on closing the gap between strategy and execution, aligning people, governance and delivery around a shared intent.

BY ARUN MANOHARAN, GLOBAL HEAD OF STRATEGY ENABLEMENT, UBDS DIGITAL

LARGE STRATEGIC transformation programmes rarely fail suddenly.

More often, they begin with clarity and momentum. The business case is approved, budgets are released, and there is a sense that the hardest work is complete. What follows is more subtle. Progress slows, pace erodes, and benefits become harder to realise as strategy is translated into projects, milestones and KPI dashboards.

There is evidence supporting this pattern. While 56% of organisations report achieving most or all of their transformation goals, only 12% sustain those gains beyond three years. This is not theoretical. It reflects a recurring reality seen across large public sector transformation programmes in the UK, where early clarity at the strategy stage often gives way to fragmentation during execution.

At its core, the challenge is structural. It is rooted in how organisations are designed: their governance, incentives, operating models and culture, and how these shape the way strategic transformation programmes are approached. Strategy is often treated as a discrete phase: created, approved and then handed over. Delivery is expected to execute against it. This sequential model is deeply embedded, yet in practice, strategy and delivery are interdependent and must continuously inform each other.

When organisations fail to address this, something critical is lost between intent and execution.

The first loss: translation

In many cases, strategy begins and ends as a document. It exists as a slide deck or business case designed to secure alignment. Once approved, it transitions into delivery artefacts intended to guide execution.

This is where the first cracks appear.

Translation is not just communication. It is the process of converting intent into decisions, trade-offs and behaviours that can survive real operating conditions. It includes not only what is explicitly stated, but also what is implied. When translation is weak, strategy becomes fragmented. Without clear ownership, different parts of the organisation interpret intent in different ways. Delivery teams, disconnected from broader objectives, optimise for task completion rather than outcomes.

Alignment at leadership level turns into inconsistency at delivery level, and coherence across the system begins to break down.

The overlooked system: people

Implementing strategy brings together fundamentally different ways of thinking. Senior leaders operate in abstraction and narrative, while delivery teams operate in specificity and constraint. Their questions differ, as do their expectations for clarity.

There is also a generational and cognitive gap that is often overlooked. If this gap is not actively designed for,

translation weakens further. Strategy becomes either too vague to act on or too rigid to adapt. This is not a failure of individuals, but of system design.

Transformation is often described as a people problem, yet the people system is rarely designed alongside it. Roles, incentives, progression and capability building are treated as secondary. Without this, behaviour change does not sustain, and transformation outcomes begin to erode.

The risk of oversimplification

Digital transformation can also fail when simplification is used to avoid complexity.

Large-scale transformation is inherently complex. It spans systems, functions, incentives and behaviours. Yet organisations often ignore the end-to-end value chain when shaping strategy. Transformation cuts across upstream and downstream dependencies and optimising one area in isolation often creates friction elsewhere.

That friction slows adoption and undermines long-term value.

Reducing complexity too aggressively creates fragility. It removes the context needed to make informed decisions during execution.

What is required instead is the ability to operate at multiple levels simultaneously — holding strategic intent and operational reality together across the value chain. This fluency cannot sit with a small group; it must be embedded across the organisation.

The illusion of agility

Another common fault line is the perception of agility.

Many organisations adopt agile ceremonies - stand-ups, retrospectives, sprint reviews - and assume enterprise agility will follow. But without changes to the underlying operating model, these rituals remain superficial.

Enterprise agility is defined by clarity of customer priorities, the ability to make decisions quickly, and the reduction of dependencies.

Many organisations adopt agile ceremonies - stand-ups, retrospectives, sprint reviews - and assume enterprise agility will follow. But without changes to the underlying operating model, these rituals remain superficial

This requires rethinking roles. Product ownership, service ownership and user experience are not add-ons, they are core capabilities that enable organisations to respond to changing technology and market conditions.

Leadership is necessary - but not sufficient

Senior sponsorship signals its importance, but without clear delegation it can create bottlenecks. Delivery teams end up with accountability but not control.

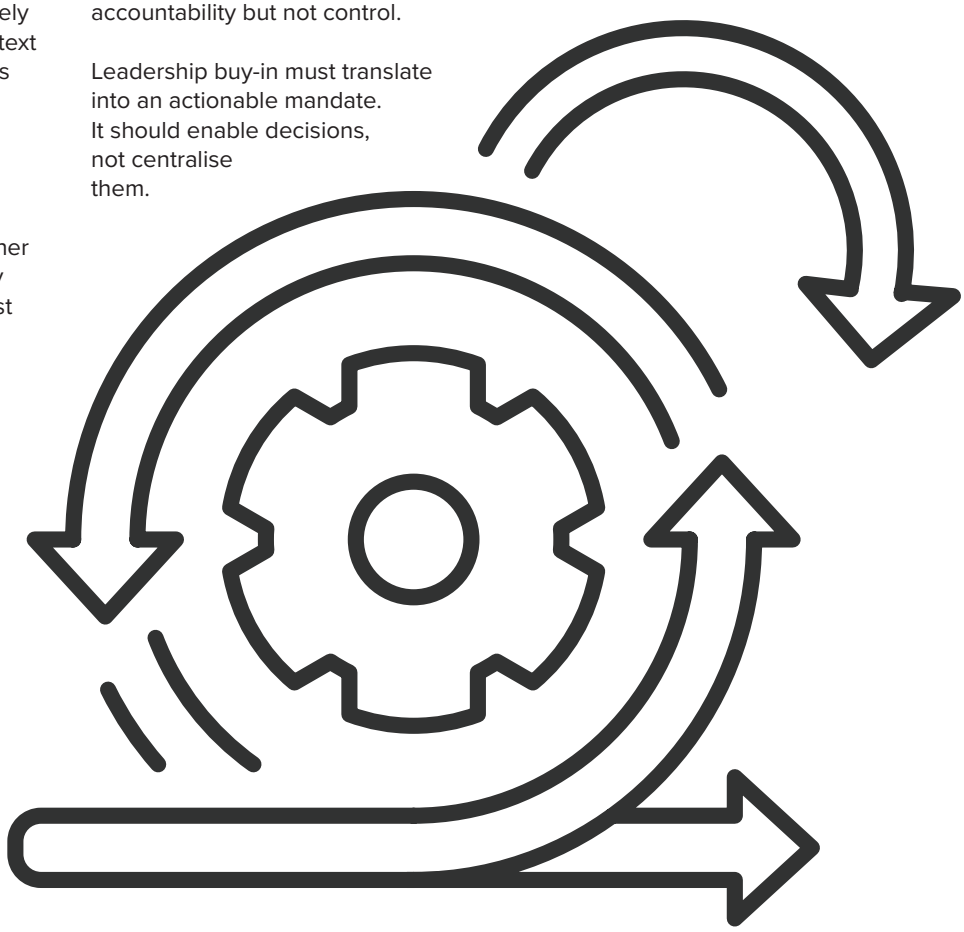
Leadership buy-in must translate into an actionable mandate. It should enable decisions, not centralise them.

In one central government organisation, this was addressed by introducing a lean project management office. This brought together representatives from across the value chain, including delivery, strategy and people functions, into a single operating layer.

Its role was not to track delivery in isolation, but to maintain continuity between strategy and execution. Translation became an ongoing process rather than a one-off handover, ensuring decisions reflected both strategic intent and operational reality.

The result was a more coherent progression from strategy to delivery, with benefits realised within expected timeframes rather than eroding during execution.

Strategy does not move linearly into execution; it evolves. Recognising this fluidity is critical. The question and focus become less about designing the perfect strategy and more about designing the conditions that allow it to survive and adapt.



The sovereignty gap UK organisations can no longer afford to ignore

Cloud strategy is entering a new era, shaped by sovereignty, resilience and geopolitical risk. For UK organisations, smarter hybrid architectures are becoming essential to balancing control, compliance and agility.

BY CHRIS CARREIRO, CHIEF TECHNOLOGY OFFICER, PARK PLACE TECHNOLOGIES

LAST YEAR, Microsoft admitted it cannot guarantee the sovereignty of data stored in its European cloud. A major AWS outage disrupted HMRC and UK banks simultaneously. Most recently, more than 70 organisations backed by the European Commission have launched EURO-3C. This federated sovereign cloud and AI infrastructure was designed to strengthen Europe's technological independence and reduce its reliance on non-European providers.

These are not isolated incidents. They are the architecture of a reckoning. For UK organisations, the assumption that underpinned the two decades of cloud adoption – that geopolitical stability and regulatory certainty would continue – no longer stands.

The question has shifted from whether to rethink cloud strategy to how quickly the underlying infrastructure can be rebuilt to support a very different future.

Why traditional cloud adoption models no longer suffice

The all-in approach to public cloud made sense in the context it was born into. Hyperscalers offered scale, speed and cost efficiency at a moment when regulation was permissive and geopolitical risk felt abstract. Enterprises outsourced complexity and concentrated dependency, and for years the trade-off was rational.

That calculation has fundamentally changed. The Competition and Markets Authority (CMA) is actively scrutinising hyperscaler dominance in the UK cloud market. Data localisation requirements are tightening. As EURO-3C demonstrates, the international consensus is shifting. Sovereign infrastructure is no longer a niche concern for government agencies; it is becoming a baseline expectation across sectors.

For UK organisations, this shift carries urgency. The events of the past twelve months have exposed what concentrated cloud dependency looks like in practice: critical national infrastructure disrupted by a single provider's outage and data sovereignty guarantees that cannot be honoured under legal scrutiny. These are not edge cases or theoretical risks. They

are operational realities that have already landed on board agendas.

Sovereignty is fast becoming a competitive advantage. Organisations that can demonstrate genuine control over their data estate will increasingly carry more weight with regulators, customers and partners than those that cannot. That means knowing where data lives, who can access it, and under what legal framework.

Moving from cloud-first to smarter, more resilient strategies

The response to this challenge is not a retreat from cloud. That framing misses the point. The organisations navigating this most effectively are not the ones rejecting public cloud outright, but the ones moving beyond the blunt instrument of a single-vendor strategy towards architectures that are fit for purpose.

Hybrid models are driving this transition. More than half of all AI workloads now run in private cloud or on-premises environments, driven by the need for greater control over sensitive data and tighter integration with core systems. AI is the forcing function here. Low latency, data proximity and regulatory sensitivity are the infrastructure requirements now exposing the limits of a one-size-fits-all public cloud approach in ways that simpler workloads never did.

In practice, smarter architecture means intelligent workload segmentation: placing data and applications based on sensitivity, regulatory requirements and strategic importance, rather than convenience or inertia. The approach combines the security of on-premises infrastructure with the agility of cloud for the workloads it genuinely suits, while maintaining unified visibility and governance across the entire estate. Single-vendor strategies are structurally incapable of delivering this. They are designed for consolidation, not differentiation.

The organisations that build this capability now will not only be better positioned for compliance — they will be building a foundation that is resilient to the kind of disruption already seen across the sector.

Building cloud architecture for uncertainty

Turning sovereignty ambitions into operational reality is where many organisations will find the hardest work. Physically relocating, migrating and re-architecting data estates at pace is a significant undertaking, driven by evolving data residency requirements, regulatory changes and the strategic need to reduce single-provider exposure. And there is a dimension to this challenge that most organisations have not yet fully confronted.

Physical infrastructure risk is the blind spot. The dependency on hyperscaler data centres creates exposure to resource volatility, energy constraints and geographic concentration that is as consequential as any digital or regulatory risk. Organisations that have built resilience frameworks around digital threats and compliance obligations but have not examined the physical dependencies beneath their cloud estate are carrying risk they may not have fully mapped.

Closing that gap requires a deliberate, layered approach: diversifying infrastructure providers, planning for residency requirements before they become enforcement actions, and stress-testing those frameworks against physical as well as digital failure scenarios.

The UK is part of a broader sovereign shift. EURO-3C is evidence of that. But the ambition is only as strong as the infrastructure built to support it. The organisations that move now will be building architectures designed for uncertainty rather than optimised for a stability that no longer exists. That will prove to be the right call.

Your security stack might be your biggest vulnerability

Complex security stacks can weaken protection. The future for channel partners lies in simpler, resilient architectures focused on control, containment and outcomes.

BY MICHAEL VALLAS, GLOBAL TECHNICAL PRINCIPAL, GOLDILOCK SECURE

ASK ANY reseller or MSSP what their solution stack looks like right now, and brace yourself. They will explain dozens of overlapping tools, each with their own configurations, dashboards, logic and alerts. They all promise next-gen protection, yet few of them align or talk fluently to each other.

That's less of a seamless security posture and more of an emerging pressure cooker when the chips are down.

Industry experts talk of tool fatigue as one of the biggest barriers to effective security. IBM research shows that organisations now manage, on average, more than 80 different security tools across nearly 30 vendors, creating fragmented visibility and making it harder to uniformly prioritise and respond to today's threats.

More tools, less clarity, different pressures

Security stacks have grown organically over time. As new threat classes emerge, new tools are added. When another threat vector appears, another layer follows, and so on. On their own, each solution may address a problem space, but collectively, they often just create new ones.

The reasoning is good, but the result can be too many alerts, too many dashboards, too many points of misalignment.

This puts channel partners in a challenging position. As the threat landscape continues to expand, it remains hard to continuously deliver clear security outcomes from widening solution stacks. When the tools signal a clear need for action, that action must come fast and be specific in the right place. The focus on rapid detection and effective mitigation action gets diverted as teams are left stitching together ever more components to handle the complexity of what to worry about and what to do.

While each solution layer might address a specific risk, they are all software-based and by definition could inadvertently hide microscopic blind spots in code or configuration that attackers will exploit through all the traditional methods of corruption, subversion, concealment and impersonation.

The necessary shift to active defence

Something is shifting in the way the channel is building solutions. Rather than continuing to layer additional tools onto already saturated environments,

forward-looking partners are beginning to rethink the stack itself.

The focus is moving toward what might be described as active defence, where the priority isn't just visibility, but the ability to act instantly and decisively when something goes wrong. The key to this is to rapidly understand the threat level justification to act, to close down an asset or segment to either validate it is clean or identify the threat and neutralise it.

With AI-driven attacks operating at machine speed, organisations are embracing an "assumed breach" mindset. While the philosophy accepts compromise as inevitable, the focus should also be on keeping the attack surface as small as possible and turning breaches into containable incidents. The leverage of advanced cyber tools is then all about rapid resolution within a contained zone.

In practice, this means cutting complexity: fewer tools, tighter integration and fewer moving parts. It also means bringing physical controls back into play, enforcing hard boundaries and instantly isolating critical assets.

Unlike software-based segmentation, a physical layer can't be bypassed by compromised credentials, zero-day exploits or misconfigured policies. By selectively connecting and reconnecting critical assets at the right time and in the right places, organisations can regain control over risk without major disruption to their day-to-day operations.

This is not to say digital defences should be abandoned. Rather, they should be enhanced and targeted, with ground-up resilience that remains effective even when the software layer has been compromised to some degree.

Regulation is reinforcing the change

Frameworks such as NIS2 in the EU, the UK's Cyber Security & Resilience Bill and DORA in the financial sector are all placing greater emphasis on resilience and containment. The expectation is no longer just that threats are detected, but that organisations can demonstrate a breach in one area won't cascade out across the network.

In other words, organisations must demonstrate control, not just visibility. That's a very different requirement, and one that complex, loosely integrated stacks have a hard time meeting.

For channel partners, this creates both pressure and opportunity. Customers are increasingly looking for advice and solutions that clearly define how to manage and reduce risk. The new "must have" is the ability to streamline architectures and physically separate systems from the network, which reduces exposure by keeping critical assets outside the view of attackers without disrupting business continuity.

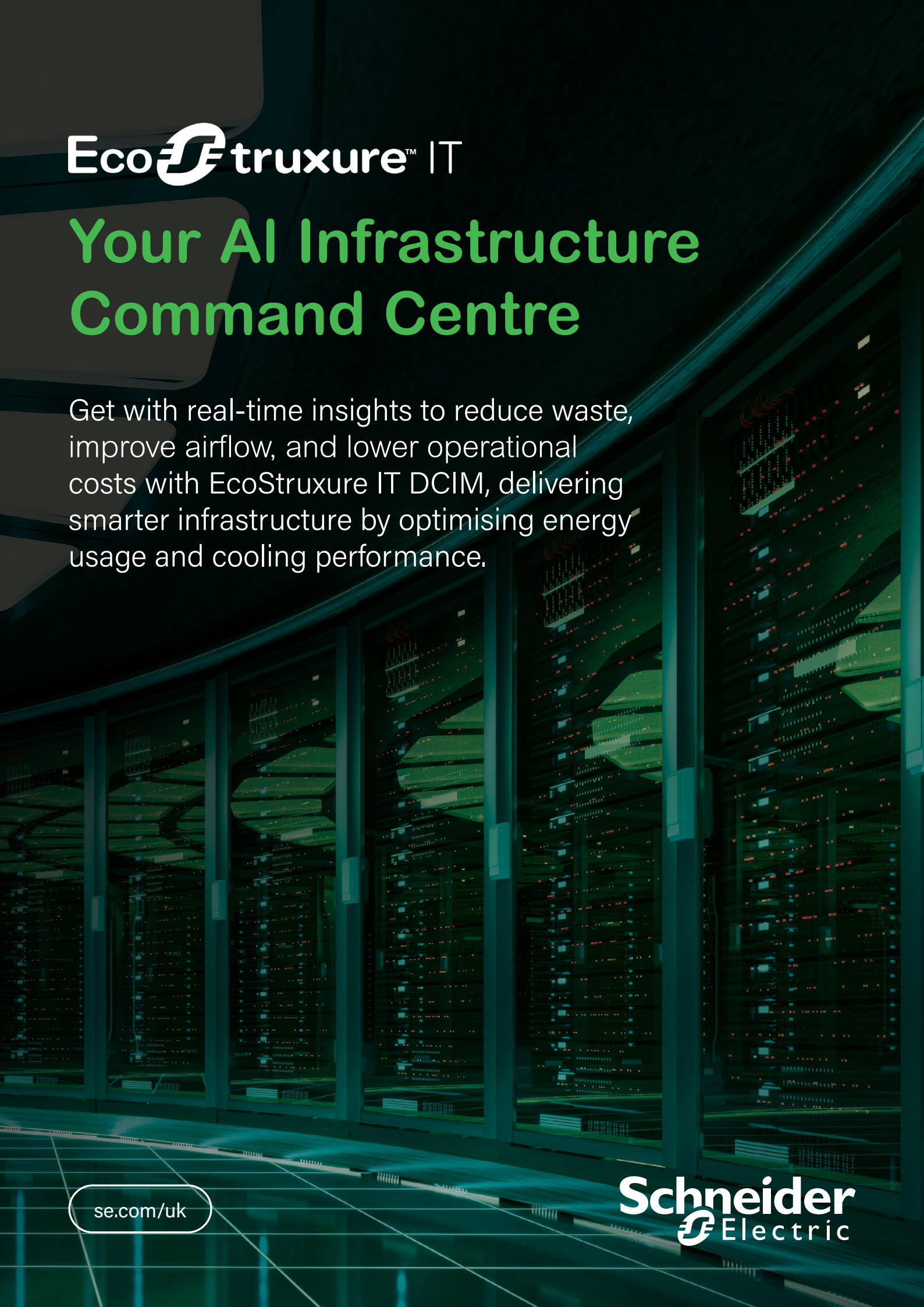
It also changes what partners can grow as value propositions. Customers are less interested in buying another layer of tooling and more focused on buying the outcomes they need to present to the Board. Such as how quickly a threat can be contained and how clearly any disruption's blast radius can be limited. That shift towards measurable protection is redefining what solid security looks like.

A strong future through simplicity

The next phase of growth in the channel won't come from adding more layers, but from giving the ones in place a more powerful purpose.

Partners who succeed will be those helping customers gain faster and more powerful attack control by rationalising their stacks and focusing on what actually improves their business operating security. This means prioritising clarity of action over coverage of marginal concerns and self-inflicted complexity.

The ultimate change is in how partners position themselves. Instead of selling another tool, the conversation becomes simpler and more outcome-focused: how to build stronger businesses that can handle the future of cyber defence needs.


EcoStruxure™ IT
Your AI Infrastructure Command Centre
Get with real-time insights to reduce waste, improve airflow, and lower operational costs with EcoStruxure IT DCIM, delivering smarter infrastructure by optimising energy usage and cooling performance.
se.com/uk
Schneider Electric