DW
DIGITALISATION WORLD

MODERN ENTERPRISE IT - FROM THE EDGE TO THE CORE TO THE CLOUD

ISSUE VII 2025

AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

DIGITALISATIONWORLD.COM

WHEN GREEN IT MEETS BUSINESS VALUE

INFINIDAT


Liquid cooling proven at exascale.
Simplified for AI at scale.
We're ready for AI. Are you?
Learn more about our end-to-end AI-ready cooling technology
Scan the QR code to learn more.
se.com/datacentre
Life Is On
Schneider Electric

VIEWPOINT

BY PHIL ALSOP
EDITOR

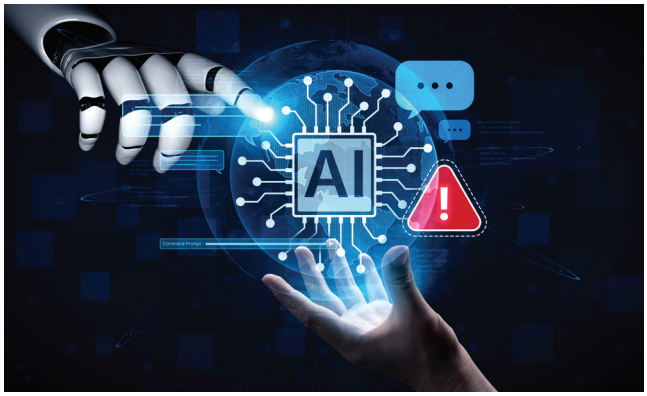
Cybersecurity, AI and risk in an autonomous era

GARTNER'S LATEST ANALYST STORIES IN THIS ISSUE underscore a profound inflection point in the relationship between technology, risk and enterprise resilience. Taken together, they reveal not just trends but the structural shifts that will define the digital economy through 2030.

The most striking theme is the shift from detection-and-response (DR) models to preemptive cybersecurity. Gartner's forecast - that preemptive solutions will command half of IT security spend by 2030, up from just 5% in 2024 - signals a decisive break with the reactive mindset that has defined the past two decades. The rise of the global attack surface grid (GASG) and the looming explosion of vulnerabilities demand autonomous, AI-powered defences. Concepts like the Autonomous Cyber Immune System (ACIS) evoke biology, where the body neutralizes pathogens before illness occurs. This metaphor is apt: in a world of agentic AI and self-learning threats, security must evolve into something more organic, adaptive and invisible.

This pivot mirrors the broader AI investment boom. With global AI spend set to reach $1.5 trillion in 2025 and $2 trillion in 2026, Gartner highlights the dual engines propelling growth: infrastructure expansion by hyperscalers, and the diffusion of AI into consumer devices like smartphones and PCs. Particularly notable is the rapid scaling of domain-specific applications, from AI for cloud-native security to generative AI-powered personal assistants, which will fragment markets and open fresh opportunities for specialized vendors.

The Hype Cycle for Emerging Technologies further contextualises this momentum. Gartner's framing of an "autonomous business era" is not hyperbole. Machine customers, AI agents, decision intelligence, and programmable money together suggest a landscape where transactions, workflows, and even strategy are executed by non-human actors. The emergence of machine customers, already three billion today, projected to reach eight billion by 2030, could rival cloud computing in its transformative potential. Organisations that fail to adapt



their business models for these algorithmic consumers risk disintermediation.

Yet, if cybersecurity and AI define the opportunities, risk reflex defines the organizational imperative. Gartner's call for reflexive risk ownership is timely: risks are increasingly interdependent, fast-moving and opaque. Building "muscle memory" for risk - through engineered systems, intentional provocation, and recognition of good behaviours - offers a human complement to the technological arms race. Without it, even the most advanced AI systems could leave enterprises brittle in the face of disruption.

What ties these narratives together is a recognition that technology no longer merely augments business, it increasingly is the business.

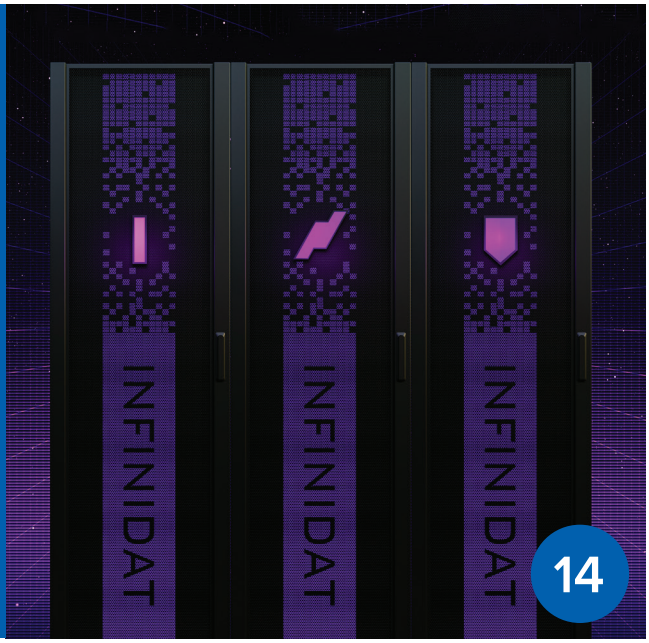
To thrive in this new era, leaders must embrace preemptive security, invest in AI with discipline, prepare for autonomous customers, and embed risk reflexes into culture. The organisations that succeed will not be those that respond fastest, but those that anticipate, adapt and trust autonomy before their competitors do.

DW DIGITALISATION WORLD

COVER STORY

When Green IT meets business value

Introducing the newly expanded InfiniBox® G4 Family



DIGITALISATION WORLD

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

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

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

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

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

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

Directors
Scott Adams: CTO
Sukhi Bhadal: CEO

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

Angel BUSINESS COMMUNICATIONS

Digitalisation World is published 10 times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication. Angel Business Communications Ltd.

ISSN 2396-9016 (Online)

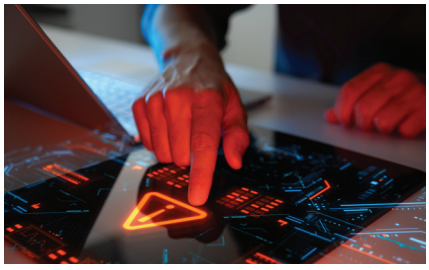
Cybersecurity skills shortage: A crisis for EMEA organisations

An escalating cybersecurity skills crisis demands a fundamental shift in organisational strategy, challenging businesses across EMEA.

A PRESSING cybersecurity skills crisis is prompting 64% of organisations in EMEA to resort to risky shortcuts and quick fixes to satisfy security demands, as highlighted in a recent report by Insight Enterprises.

In the UK, the issue is equally alarming. A substantial 67% of organisations acknowledge a cybersecurity skills gap, with over half describing the repercussions as "severe" or "significant." The scarcity most affects senior roles, with 50% reporting deficiencies in strategic skills such as governance, planning, and risk assessment.

Across EMEA, just 24% of IT decision-makers affirm that their in-house cyber skills are sufficient to counter evolving threats. These shortages are stalling critical initiatives (57%) and ensuring that more than half toil to meet compliance mandates.



The report identifies primary barriers to bridging the skills gap in EMEA:

- 68% of IT leaders blame the high costs associated with hiring and training.
- 65% point to a dearth of qualified candidates available in the market.

Simplifying the dilemma to recruitment fails to capture the full scope. The cyber skills shortage is not merely a technical gap; it spans operations, leadership, and compliance, undermining resilience and long-term planning.

Cybersecurity has evolved past a staffing dilemma—it is now a strategic concern. As organisations hasten digital transformation, the widening cyber skills gap is shaking confidence in their secure innovation capabilities. It's more than a talent issue; it's a threat to sustained growth and resilience.

Insight EMEA President Adrian Gregory emphasised a fundamental evolution in approach, stating that successful organisations are those that " align strategic talent with intelligent technology and trusted partnerships" The key lies in leadership adept at orchestrating human–machine synergies, translating technical risks into business impacts, and embedding security in innovation.

Thus, the challenge extends beyond recruitment. It calls for a reimagining of leadership approaches to cultivate resilience and maintain a competitive edge.

Report reveals industry challenges in digital trust

SECTIGO, a key player in digital certificates and Certificate Lifecycle Management (CLM), has launched its inaugural State of Crypto Agility Report, co-researched with Omdia. The report delves into enterprises' readiness for two seismic reforms in digital trust: the revolutionising of SSL/TLS certificate lifespans to a mere 47 days by 2029 and the fast-approaching shift to post-quantum cryptography (PQC) by 2030.

Tim Callan, chief compliance officer at Sectigo said, "Today, certificates are front and centre in the fight to secure our digital future. Building certificate agility now is the fastest path to achieving the crypto agility required for post-quantum cryptography readiness later."

Organisations face formidable challenges with both transformations individually. With both coming together a new approach must be devised. 90% of companies recognise a symbiotic relationship between prepping for short-lived certificates and PQC readiness, with transitioning to 47-day certificates seen as a critical gateway to PQC adoption. However, organisational readiness for either issue is low.

The key findings of Sectigo's research are:

- 47-day SSL/TLS certificates
- 96% of firms express concerns over the impact of shorter SSL/TLS certificate durations on operations.
- 19% report feel fully prepared for the shift to the 47-day renewal cycle.
- 5% have embraced full automation in certificate management, leaving the vast majority reliant on manual processes, heightening operational risk as renewal frequencies escalate.
- PQC migration
- 98% of organisations anticipate facing hurdles with PQC implementation, whilst 92% expect barriers during the transition.
- Just 14% have conducted a thorough assessment of systems vulnerable to quantum threats.
- Only 15% feel utterly confident in integrating PQC without major disruptions.

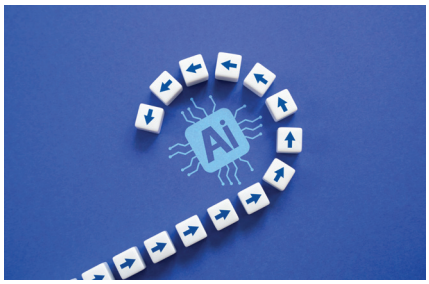
AI adoption wavers among large enterprises

Recent data reveals a slight dip in AI adoption, pointing to strategic reevaluations among major companies.

AI ADOPTION within large enterprises has seen a slight drop, falling from 14% to 12% over recent months, according to data from the US Census Bureau. This trend suggests a momentary hesitance among larger organisations, perhaps due to unclear returns on substantial investments.

While the broader trend remains positive, the minor decline points towards frustrations over returns on substantial investments, such as cutting-edge data centres and extensive AI supports.

The US Census Bureau's biweekly surveys, canvassing 1.2 million companies, notes an overall growth in AI use. Currently, 9.7% of participants reported utilising AI recently, up from 8.8% previously. Anticipations over the coming six months also rise, with 13.7% preparing for AI adoption in production roles. Despite this, two-thirds of companies remain tentative, showcasing a selectively wider integration period ahead.



Industry leaders underline the critical importance of tailored strategies in securing successful AI integration. Sheila Flavell CBE, COO of FDM Group, articulates "The dip in AI adoption doesn't mean companies are abandoning AI altogether - it shows the rolling our the tech without the right training and strategy won't work. AI can only deliver value when people know how to use it effectively."

Meanwhile, Andy Ward, SVP International of Absolute Security, highlights a gnawing concern over vulnerability, stressing the need for robust deployment strategies. His insights underline that a blanket approach without real-time oversight risks amplifying vulnerabilities rather than plugging them."Now is the time for security leaders to ensure their people, processes, and technologies are aligned, or risk being left dangerously exposed."

Experts argue that the Census data might diminish the true scope of AI application, noting its broader use beyond production to administrative, marketing, and customer service functions. Regardless, adoption seems poised to surpass early e-commerce benchmarks within a similar timeframe, according to analysts.

Torsten Sløk, chief economist at Apollo Academy, indicates a cautious approach by larger entities, while Arpit Gupta at NYU Stern advocates "trillions in AI capex should probably be reconsidered". Observations from MIT further reveal that 95% of firms grapple with attaining financial returns, sparking discussions on a looming AI "bubble".

Gen AI adoption: A new era for enterprises

THE RECENT Capgemini Research Institute report, 'Harnessing the value of AI: Unlocking scalable advantage,' delves into the fast-tracked adoption of generative AI (Gen AI) across enterprises. The findings indicate a palpable shift toward embedding AI as active team members or even supervisors for other AI systems, forecasting such integration within 60% of organisations in the next year.

However, the transition isn't without hurdles. Many companies acknowledge gaps in their preparedness for dynamic human-AI synergy, with two-thirds recognising a need to revamp their team structures.

In its third annual edition, the report underscores a glaring escalation in Gen AI adoption: a significant leap to 30% of firms fully or partially scaling Gen AI, climbing fivefold since 2023. Roughly 93% are keenly involved in exploring or enabling Gen AI by 2025.

Leading sectors embracing this tech transition are telecom, consumer products, and aerospace, focusing primarily on functions like customer operations and marketing.

Franck Greverie of Capgemini articulates a need for strategic data environment establishment to truly leverage the benefits of AI, pointing to the advantages of a balanced human-AI chemistry for favourable outcomes. The momentum behind investment is clear, with around 79% of organisations content with the tangible outcomes from Gen AI investment. A notable 88% have increased their AI investments by an average of 9%, with predictions of further allocation increases within Gen AI.

Momentum is building around AI agents, with increasing adoption across product design, marketing, and sales. Around half of those scaling AI agents are also engaging with multi-agent systems, with anticipation of a more autonomous, self-learning trajectory.

AI's role in revolutionising cybersecurity

Arctic Wolf's report reveals AI's pivotal role in evolving security operations, with 99% seeing it influence upcoming cybersecurity investments.

ARCTIC WOLF®, a global leader in security operations, recently unveiled insights from its latest report Navigating the Human-AI Relationship for Security Operations Success. Conducted in collaboration with Sapio Research, the study surveyed almost 2,000 IT and security decision-makers worldwide. Astonishingly, 99% asserted the influence of AI on cybersecurity purchases or renewals in the coming year.

Modern security teams are inundated by a deluge of alerts originating from fragmented tools and disparate data sources.

With finite staffing and resources, they face high-pressure decisions on which alerts warrant investigation. This often leaves critical threats obscured by the noise leading to analyst burnout, prolonged response times, and increased vulnerability.

Such mounting pressure has positioned AI as a pivotal element in cybersecurity strategy. Organisations are embracing AI not merely as a tool, but as a strategic partner in security operations.

From advanced threat detection and large language model assistants offering contextual insights, to AI-driven workflows automating mundane tasks, AI is integral. Coupled with skilled human oversight, these tools can distinguish genuine threats, mitigate alert fatigue, hasten investigations, and ensure focus on primary risks.

Key findings from the report highlight:

- AI as a Cybersecurity Staple: With 99% affirming AI's impact on security decision-making, and four in ten budgets allied to AI solutions.
- Widespread Adoption: 73% of organisations have adopted AI in their cybersecurity framework, spearheaded by the U.S. (82%) and financial services (82%). Meanwhile, sectors like utilities (59%) and regions such as the Nordics (59%) proceed cautiously.
- Automation Transforming Security: 73% plan to deploy AI in security automation, with 72% focusing on threat prediction and prevention and 70% enhancing detection capabilities.
- Essential Human Oversight: Over two-thirds argue for significant human input in AI processes, 52% intend to upgrade team skills for AI management, and 46% foresee analysts validating AI alerts.
- Challenges to Overcome: Data privacy poses the top challenge at 33%, followed by cost issues (30%) and fulfilling organisational needs (28%).

"Artificial intelligence is rapidly becoming a cornerstone of modern cybersecurity, but it benefits from human expertise to be truly effective," said Dan Schiappa, President of Technology and Services at Arctic Wolf. "The insights from this report give leaders the data they need to make smart, targeted investments, deploying AI where it can deliver measurable outcomes, cut through alert noise, and help security teams work with greater speed, accuracy, and confidence."

Such mounting pressure has positioned AI as a pivotal element in cybersecurity strategy. Organisations are embracing AI not merely as a tool, but as a strategic partner in security operations. From advanced threat detection and large language model assistants offering contextual insights, to AI-driven workflows automating mundane tasks, AI is integral

MSP CHANNEL AWARDS 2025

CELEBRATING 16 YEARS OF SUCCESS

34 Categories across 5 Themes

3 DECEMBER 2025

LEONARDO ROYAL HOTEL LONDON CITY

KEY DATES:

3 DECEMBER: AWARDS CEREMONY

HEADLINE SPONSOR

EXAGRID®

CATEGORY SPONSORS

HORNETSECURITY

Schneider Electric

SILVER SPONSOR

Gamma

SPONSORSHIP PACKAGES

As a sponsor of the MSP Channel Awards you will gain significant marketing and branding opportunities. Sponsors are at the forefront of the awards marketing program from now until the ceremony itself in December 2025.

BOOK YOUR TABLE

Don't forget to book your table for the Awards evening. It's a great way for your company to celebrate in the run-up to Christmas.

For sponsorship opportunities and/or to book your awards table please contact:
awards@mspawards.com or call +44 (0)2476 718970

VOTE HERE: https://mspawards.com/vote

Angel BUSINESS COMMUNICATIONS

ANGEL EVENTS

Bridging IT gaps in emerging technology

Unisys's report reveals the disconnect between ambition and IT preparedness and highlights the necessity for modernized infrastructure to embrace emerging technologies.

UNISYS, a major player in global IT solutions, has published a revealing global report on how businesses are re-aligning IT strategies to integrate emerging technologies like generative AI, agentic AI, and quantum computing.

Aptly named "From Complexity to Clarity: Modernizing Cloud and IT for What Comes Next," the study sourced insights from 1,000 C-Suite professionals and IT executives spanning eight diverse global markets. The report uncovers a concerning dichotomy between ambitious business goals and insufficient IT frameworks — showcasing potential pitfalls like squandered investments, lagging innovation, and heightened cybersecurity risks. Notably, it identifies a distinguished segment, the "Innovation Leaders," exemplifying optimal IT infrastructure strategies to ignite innovation.

Key Insights:

- Majority of organisations (78%) are set to amplify investment in genAI, while 73% consider agentic AI pivotal in maintaining a competitive edge.
- Only a meagre 36% express readiness for large-scale AI workloads.
- A sizeable 82% view cloud and IT as revenue generators, with significant numbers dissatisfied with ROI on cloud technologies yet poised to elevate their investment.
- A mere 14% acknowledge preparedness for post-quantum cryptography amid rising modern cyber threats.
- An astounding 85% classify their cybersecurity stance as reactive, despite soaring downtime costs.

According to Manju Naglapur, senior vice president and general manager of Cloud, Applications & Infrastructure solutions at Unisys, an immediate overhaul in infrastructures is essential

to harness the capabilities of these groundbreaking technologies fully.

Executives consistently view technologies like agentic AI, quantum computing, and genAI as integral to prolonged success. Alarmingly, 73% warn that neglecting agentic AI could jeopardise competitiveness, prompting 82% of innovation leaders to allocate over 6% of IT budgets towards genAI technologies. This confidence is mirrored by 78% of organisations poised to increase their genAI investment, indicative of its burgeoning potential to foster innovation and strengthen competitive stance.

In spite of bold steps towards technology adoption, there's a consensus that current infrastructure lags. Over time, this scenario remains unchanged, revealing that obsolete infrastructure, talent deficits, and misalignment between business and IT persist as top hurdles in the cloud domain. For IT executives, the forecast remains bleak with readiness levels waning for quantum computing and comparable technologies.

Addressing these barriers is paramount for organisations wishing to leverage the complete potential of modern technologies through strategic infrastructure modernisation and heightened alignment with business objectives.

The infrastructural gap not only stifles innovation but aggravates security vulnerabilities. Recent data discloses that 17% experienced a breach within the past year, incurring downtime costs of up to $500,000 per hour. Furthermore, just 14% feel armed for post-quantum cryptography, underlying future cyber threats' implications.

While organisations grudgingly admit their reactive cybersecurity position, a promising 62% are either adopting or in the throes of adopting Zero Trust models — a significant 61% focusing on cyber recovery innovation, yet a scant 43% embracing AI-led cybersecurity solutions.

This window of opportunity could be pivotal in reinforcing defences as emerging technologies continue to add complexity.

Leading the charge: GPUs powering the explosive AI data centre growth

The rise of AI data centres, known as 'AI Factories', highlights the critical role of GPUs in today's tech landscape.

AS NATIONS across the globe ramp up investments in AI data centers and cloud computing, the term "Sovereign AI" is gaining popularity. These centres, often referred to as "AI Factories", are creating a surge in demand for highly specialised computing chips, particularly GPUs (Graphics Processing Units). A report by IDTechEx highlights the trajectory of AI chips, forecasting significant growth in the next decade.

GPUs are becoming indispensable, capturing a whopping 82% of the AI chip revenue in 2024. By 2025, their deployment is expected to multiply, dominated by industry leader NVIDIA with its Blackwell GPUs. Close on its heels, AMD competes fiercely with its MI300 and MI350 series, securing substantial deals with major technology companies.

Initially developed in the 1970s for basic 2D graphics rendering, GPUs have undergone significant transformations. The 1990s witnessed a growth in 3D graphics, with AMD and NVIDIA developing technologies that allowed GPUs to harness parallel processing capabilities for broader uses, such as simulations and image processing by the mid-2000s.

The surge of interest in AI in the 2010s, propelled by models like AlexNet and ResNet, further cemented the role of GPUs in training advanced AI models. Modern-day GPUs are tasked with facilitating complex AI operations, ensuring high-speed processing and supporting vast library functions needed for deep learning.

Comprised of thousands of cores, each GPU is designed to execute specific instructions simultaneously across numerous data points. Despite their simpler cache systems compared to CPUs, GPUs enhance throughput efficiency, crucial for tasks involving extensive data calculations.
The future will likely see high-performance GPUs adopt advanced transistor nodes, such as 2nm, a move that promises greater efficiency and

density. However, challenges persist, particularly with the considerable costs of ultra-advanced lithography equipment and other hurdles, such as increasing heat production and materials limitations.

Such innovations increase transistor counts and improve yield rates, though often at the cost of memory speed. High-bandwidth memory technologies, led by Samsung, SK Hynix, and Micron, are widely adopted. This ensures the necessary memory to train expansive AI models, with Chinese enterprises now entering the HBM production arena. As this industry continues evolving, GPUs are poised to play a central role in shaping the future of AI data centres.

AI cluster networking: Paving the way for a transformational 2025

KEYSIGHT TECHNOLOGIES, INC. and Heavy Reading have shared a pivotal 2025 report on AI cluster networking. As artificial intelligence adoption outpaces infrastructure development, telecom and cloud providers are urged to pivot from expansion to optimisation to handle next-generation AI tasks.

AI growth in various industries increases demands on data centres. However, traditional expansion initiatives seem inadequate. A significant 62% of respondents prefer maximising current infrastructure over new investments. This prompts operators to embrace performance optimisation strategies, such as real-world AI workload emulation to validate and enhance deployment efficiency for AI clusters.

The report, which drew insights primarily from industry respondents, showed 89% planning to either expand or maintain AI infrastructure investments. The predominant factors propelling this trend include cloud integration (on the rise at 51%), faster GPUs' deployment (49%), and high-speed network upgrades (45%).

The research highlights a transformation in industry thinking: it's no longer solely about infrastructure capacity but about optimising efficiency and reliability. As sophisticated AI models become mainstream, the importance of real-world AI workload emulation is underscored, offering a way to unlock infrastructure potential while managing costs.

"AI data centres are reaching a tipping point where performance and scale alone are not enough. Operators need deeper insight, tighter validation, and smarter infrastructure choices," explained Ram Periakaruppan, Vice President and General Manager, Network Applications & Security Group at Keysight, indicating the criticality of optimising networks in the AI era.

Businesses must prioritise soft skills for successful AI integration

AI investments thrive when paired with soft skills. Analytical and ethical capabilities unlock AI's true potential.

AS BUSINESSES intensify their AI investments, merely having technical prowess is no longer sufficient for achieving total success. Recent research from Multiverse indicates that the inclusion of soft skills—analytical reasoning, creativity, systems thinking, and ethical awareness—are critical to realising AI's full potential.

Analytical reasoning empowers employees to distil complex data, enabling AI to produce more insightful outcomes. Furthermore, it equips staff to discern instances where AI is unsuitable.

Meanwhile, systems thinking allows individuals to recognise patterns in AI behaviour and predict its responses, thus proving crucial during AI's implementation and refinement phases.

The early adoption stages of AI greatly benefit from creativity, which encourages staff to explore novel use cases and expand AI's capabilities in supporting their work.

The research highlights the necessity for ethical awareness in AI operations. Employees with these skills can identify biases in AI outputs, enforce ethical standards in deployment, and ensure that the system aligns with appropriate cultural and geographic norms.

Accenture's findings complement Multiverse's insights, suggesting that companies emphasising soft skills nearly double their chances of successful AI adoption.

Recognising culture as a primary hurdle in digital transformation, Multiverse urges business leaders to view AI as both a human and technological challenge.

"Leaders are spending millions on AI tools, but their investment focus isn't going to succeed. They think it's a technology problem when it's really a human and technology problem," said Gary Eimerman, chief learning officer at Multiverse. "Without a deliberate focus on capabilities like analytical reasoning and creativity, as well as culture and behaviors, AI projects will never deliver up to their potential.

Sheila Flavell, COO of FDM Group, commented: "Knowing how to use AI is no longer just about technical know-how - it's about adaptability, communication, and the confidence to work alongside intelligent systems, and these 'soft skills' are essential to unlocking AI's full potential within businesses.

The trajectory of AI's success is set by human oversight. AI, rather than replacing people, enriches those capable of judicious use.

Creating a digitally savvy workforce calls for governmental and industry collaboration to upskill individuals, equipping them with the requisite training to adeptly manage and oversee AI.

SNIA unveils Storage.AI, an open standards initiative for streamlining AI workloads

SNIA launches Storage.AI to tackle AI data challenges through collaborative, industry-standard solutions.

1 month ago Posted in AI Data Analytics

SNIA, a global non-profit organisation specialising in data technologies, has introduced Storage.AI™ - an open standards initiative designed to enhance the efficiency of AI-related data services. By adopting industry-standard, non-proprietary approaches, Storage.AI aims to optimise the performance, efficiency, and cost-effectiveness of AI workloads.

The initiative has garnered support from notable industry leaders, including AMD, Cisco, DDN, Dell, IBM, Intel, KIOXIA, Microchip, Micron, NetApp, Pure Storage, Samsung, Seagate, Solidigm, and WEKA. Further collaboration is planned with SNIA's partners, such as UEC, NVM Express®, OCP, OFA, DMTF, and SPEC.

AI workloads are complicated by various challenges, including latency, power, space, cooling, memory, and cost issues. The open industry effort proposed by Storage.AI offers a rapid pathway to optimising these constraints through a neutral industry initiative. By creating an open ecosystem, Storage.AI will focus on overcoming significant challenges in processing and accessing data for AI workloads. The unity among founding members reflects a shared objective — to accelerate AI adoption by filling existing gaps in data handling.

MANAGED SERVICES SUMMIT MANCHESTER

18.11.2025

MANCHESTER CENTRAL
MANCHESTER UK

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

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

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

INDUSTRY INSIGHTS

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

NETWORKING OPPORTUNITIES

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

INTERACTIVE EXPERIENCES

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Angel BUSINESS COMMUNICATIONS

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

ITEUROPA

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

https://manchester.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS ITEUROPA ANGEL EVENTS

When Green IT meets business value

Introducing the newly expanded InfiniBox® G4 Family.

BY ERIC HERZOG, CMO INFINIDAT

OVER the last 18 months, Infinidat has seen outstanding success with the launch and acclaim of the inaugural InfiniBox® G4 Family. Our goal was to create a new foundation for the future and we certainly achieved that, by providing comprehensive enterprise storage solutions that perform up to 2.5X better than the previous generation. We've made high-end enterprise storage accessible to the broadest possible range of enterprises, extending the capabilities of the award-winning InfiniBox G4 to upgrade enterprise data infrastructures without any disruption.

And the timing of this innovation couldn't have been more critical, as rising AI adoption combined with escalating Green IT agendas is placing greater demands on CIOs, CTOs and IT managers to balance the need for storage capacity with their consumption of energy resources. Now, the arrival of Infindat's expanded G4 family marks a clear step towards creating a suite of ultra efficient enterprise storage solutions, that operate at the intersection of environmental responsibility and ensuring a sustained business advantage.

Most significantly, our latest solutions include a revolutionary new smaller form-factor model: the InfiniBox™ SSA G4 F24 all-flash family. This delivers high-end storage in a reduced footprint with superior Green IT power-efficiency and at a lower entry price point for a high-end enterprise storage solution. Enterprise customers and service providers can now store larger quantities of high performance data more efficiently, have easier access to advanced storage capabilities, can benefit from flexible capacity management, free up rack space and floorspace, and reduce their energy consumption. It's green storage infrastructure offered at the best possible power to cost-efficiency ratio per terabyte of storage. In fact, our new solution is the most environmentally and commercially sustainable enterprise storage ever launched by Infinidat. It offers:

- 31% smaller physical configuration for a more efficient power profile with 28% more capacity in the smaller footprint
- 29% lower entry price point than the original small form-factor of the InfiniBox SSA G4
- 45% reduction in power per petabyte (PBu) – this means less power and coolant consumption with lower greenhouse gas emissions
- Up to 2X better bandwidth performance and 32% greater overall performance.

Scale with more flexibility

In addition, to address evolving enterprise customer needs and provide flexible yet precise enterprise storage, InfiniBox SSA has shifted from a "partially populated" model to a new "scale-up" model. This fundamentally alters how customers can expand their storage solutions. Rather than being restricted by pre-determined 20% capacity increments (60%, 80%, 100%), the new InfiniBox SSA models provide more flexible and fully non-disruptive

upgrade capacities and options in smaller upgrade increments and at lower pricing per upgrade.

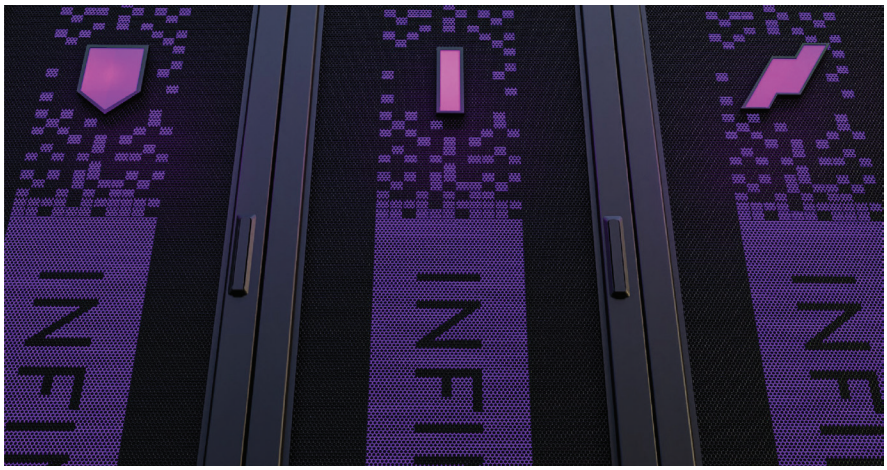
Independent analyst endorsement

Analyst group IDC has stated that the business impact for enterprises implementing Infinidat's solutions shows a clear financial return on their investments. Through a series of in-depth customer interviews and a proven methodology for determining business value, IDC's 2023 Business Value analysis found that these enterprises realised significant value from their Infinidat solutions, with clearly quantifiable benefits. IDC's analysis found that annual average benefits for Infinidat's enterprise customers were in the region of $1.29 million ($166,700 per PB) – approx. £1m and £125,000 per PB – with a 162% five-year return on investment (ROI) and payback within 11 months.

On Infinidat's latest InfiniBox G4 and InfuzeOS enhancements, IDC's Worldwide Infrastructure lead and Group Vice President, Ashish Nadkarni, stated: "Infinidat is delivering all the right things in their latest enhancements for the InfiniBox G4 family – higher efficiency, Green IT, reduced entry price point, more flexible scaling options, larger capacity in a more compact form-factor, and expanded native protocol support with the addition of object/S3. In 2024, Infinidat delivered a very innovative enterprise storage solution that set new benchmarks with the InfiniBox G4. In 2025, the progression of the G4 is extending the reach of the G4 beyond existing customers and into new enterprise customers. Infinidat is making it easier for large enterprises to deploy the InfiniBox G4 for a broader range of applications and workloads." A powerful reaction to our latest solutions.

Holistic lifecycle approach to sustainability

The most significant additions to the G4 family are the range of energy efficient enhancements conceived by our product development experts that have a direct impact on reducing energy resource consumption. Data centres worldwide are having huge issues with power, cooling and rack space, a problem that is compounded by demand for AI applications. Infinidat has approached the issue with a design led solution that incorporates EU



EcoDesign regulations for data storage products and integrates environmental considerations into every stage of our product lifecycles, from design to end-of-life.

To stay at the leading edge of Green IT developments, Infinidat actively monitors environmental and sustainability regulations across the globe to ensure our manufacturing is aligned with local and national requirements. The new G4 family design surpasses earlier solutions with its emphasis on three core dimensions of environmental sustainability. Firstly, reparability - products are designed to be fully disassembled for repairs or reuse purposes. Secondly, energy efficiency - our solutions' active state has the lowest possible power consumption without compromising quality and security efficiency. This included a shift in 2024 to using titanium and platinum-level certified power supplies, which have the highest energy efficiency rating. Thirdly, reliability - the maximum system operating temperature was increased to 35 degrees Celsius, ensuring that our systems are reliable in a wider range of operating environments with a reduced requirement for additional cooling infrastructure.

Prioritising the E^2 Factor

In addition to this, our advanced enterprise storage systems, such as our InfiniBox and InfiniGuard® solutions, are designed to provide the highest possible performance footprint, further enhancing our environmental credentials. They store larger quantities of data more efficiently, which frees up rack and floorspace, with a lower energy consumption (kW) and carbon footprint. In short, customers have increased storage capacity but use fewer storage arrays and they have reduced power, cooling and resourcing costs per TB of storage.

We've called this approach the "E^2 Factor" because it delivers both environmental and economic benefits. What is good for the environment translates directly into excellent economic benefits for an enterprise. Our storage solutions perfectly balance capacity and real world application performance needs with the requirement to minimise floorspace, power/cooling costs, and carbon footprint. And customers save money

We've called this approach the "E^2 Factor" because it delivers both environmental and economic benefits. What is good for the environment translates directly into excellent economic benefits for an enterprise. Our storage solutions perfectly balance capacity and real world application performance needs with the requirement to minimise floorspace, power/cooling costs, and carbon footprint

through lower CAPEX and OPEX, with a data centre that is more energy efficient and more environmentally friendly.

Best of all, customers can measure these improvements directly using InfiniVerse®, a cloud-based, AI-driven platform that provides advanced dashboard monitoring, predictive analytics, and single interface support for all InfiniBox systems, wherever they reside in the customer's estate.

Customers can view environmental data, such as power consumption over time, system temperature and storage utilisation, and take ownership of their energy consumption to support wider Green IT initiatives. When customers become aware of how much power their storage is consuming, they will often discover that the actual rate is 20% less than the maximum levels shown in technical specs. They can set their own energy reduction targets and make further efficiency savings. We can capture historical power consumption (kW) and CO2 emissions (kg/hr) of the Infinidat estate, which allows customers to determine power usage and carbon footprint and measure their internal Green IT initiatives or SLAs. Alongside reduced energy utilisation is floorspace. Data centre estate costs have risen dramatically and because the InfiniBox G4 stores larger quantities of data more efficiently, this frees up additional rack and floorspace.

Proven track history

We have a history of consolidating other vendors' arrays into Infinidat power-efficient arrays. For example, a Global Fortune 500 Financial Services company replaced 288 floor tiles of a competitor's all-flash product with only 61 floor tiles of the InfiniBox SSA all-flash array solution, running all the same workloads and applications.

In another example, a Global Fortune 500 Food Distributor replaced 27 competitor arrays with 4 InfiniBoxes. Consolidation reduces the number of racks, floor tiles, and overall power and cooling costs. This results in a lower total cost of ownership (TCO) and reduced environmental impact of your IT infrastructure.

This ability to consolidate also extends to the InfiniBox Hybrid platform as a powerful backup target device. In one of our Fortune 500 enterprise customers, Infinidat replaced 38 of a competitor's purpose-built backup appliances with 20 InfiniBox Hybrid solutions.

This customer experienced a 50% CAPEX saving on their initial purchase, achieved all backup window and recovery SLAs, which the competitor had been unable to meet, and saved in the first year $1.5M in OPEX savings. Another example of how we reduce floor tiles, and the associated power/cooling and carbon footprint.

Our commitment to operational decarbonisation

One very clear way that enterprise buyers can assure themselves they are making inroads with their Green IT programmes is to prioritise vendors like Infinidat that are taking this seriously inside their own enterprises. Infinidat has made a large, top-to-bottom commitment across all its operations to reduce/remove its carbon footprint and the associated greenhouse gases. To demonstrate this, our key initiatives include:

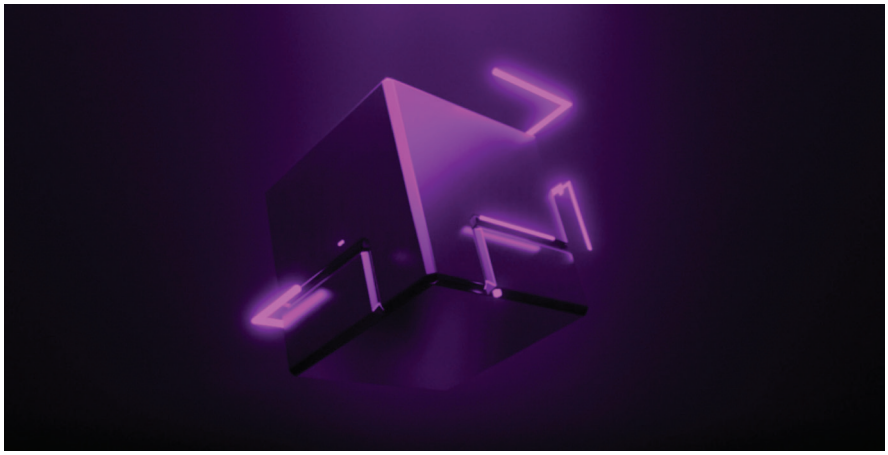
- **Integrating ESG Reporting:** Environmental, Social, and Governance (ESG) principles are incorporated into every part of Infinidat's operations, from supply chain management to technology development.
- **Reducing Scope 3 Emissions:** Infinidat has achieved a 41% reduction in total carbon footprint across its value chain, encompassing Scope 3 emissions.
- **Developing Power-Efficient Products:** Infinidat continuously upgrades its product line to deliver higher performance with lower energy consumption, as we have evidenced by the InfiniBox G4 in May 2024, and the continued evolution of this family.

InfiniBox G4 F24ST SSA takes this even further proving that sustainability and performance go hand in hand. By embracing the E^2 Factor - optimising environmental and economic benefits - our solutions deliver more capacity with less power, cooling and floorspace.

From design through to operations, we're committed to reducing carbon footprints, while lowering TCO and ensuring enterprises can achieve their Green IT goals without compromise.

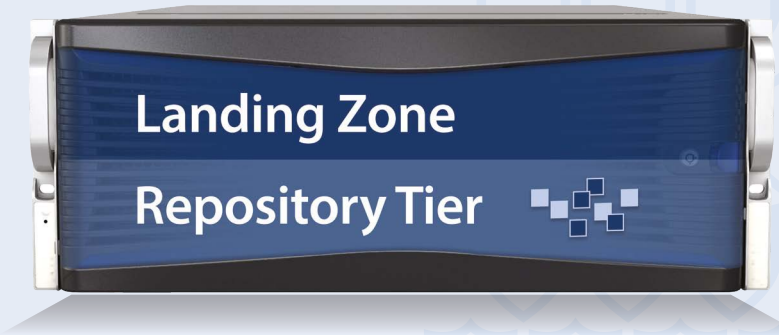
The launch of Infinidat's expanded G4 storage family exemplifies that Green IT and enterprise grade storage performance are inseparable. In an industry where scaling usually means more arrays, more racks and more power – our latest launch of products demonstrates that a different pathway does exist. One that offers more capacity, more flexibility and more performance but consumes fewer resources, less floorspace and energy. G4 is more than an enterprise storage solution - it's a strategic move towards greener, leaner and smarter IT operations.

www.infinidat.com



EXAGRID®

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

WINNER
SDC AWARDS 2023

- **Storage Company** of the Year
- **Backup/Archive Innovation** of the Year

Thank you so much to all who voted, and congratulations to our fellow SDC Awards 2023 winners!

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

LEARN MORE >

Agentic AI to dominate IT budget expansion

Year-over-year spending, between 2025 and 2029, for Artificial Intelligence (AI), will grow by 31.9%, according to data from the International Data Corporation's (IDC) Worldwide Artificial Intelligence IT Spending Market Forecast. This investment, driven by the growth of Agentic AI-enabled applications and systems to manage agentic fleets, will reach $1.3 trillion in 2029.

THE RESEARCH reveals an unprecedented surge in Agentic AI spending and signals a transformation within enterprise IT budgets—especially when it comes to software—to investment strategies led by products and services based on an agentic AI foundation. This conversion is further supported by anticipated growth in platform solutions that enable companies to build, manage, and operate their agents more securely and efficiently.

"An important takeaway from this forecast is the clear alignment between the growth in (AI) spending and IT leaders' trust that effective use of AI can boost future business success," said Rick Villars, group vice president, Worldwide Research at IDC.

"Application and Services providers that are behind in putting AI into their products and not extending them with agents are risking market share losses to companies that made the decision to put AI at the center of their product development roadmap."

Key Research Highlights

- **Infrastructure Build Out Continues -** through 2029, service providers will account for 80% of infrastructure spend as they support massive increases in agentic workloads.
- **Agent Construction & Control -** a logarithmic (10x) increase in the number and complexity of 3rd party and custom-built AI agents used by enterprises in the next five years.
- **App AI-Enablement Accelerates -** spending on AI-enabled applications will increase faster than any segment, triggering major competitive shifts in the software industry.
- **AI IT & Business Services –** services providers will be the most profoundly affected as enterprises boost spending on agentic AI thus transforming IT business services.

AI: A test of innovation and leadership

The forecast also indicates that the adoption of agents and Agentic AI will accelerate innovation in how companies use technology and code to transform their business. These investments and the evolution of related products will increasingly determine the success or failure of the business and tech leaders who put them in place, and the businesses that use them. For this reason, informed leadership will be critical to success during these next several years.

"This research reveals several important issues for businesses to consider about the interconnection between labor and AI investment," said Crawford Del Prete, president at IDC. "As an example, business leaders will need to pay particular attention to employee roles in an enterprise, and how roles change as agents become more commonplace in business. Agents will change the nature of work, making some roles highly productive, and others obsolete. Workers and enterprises will need to be more agile than ever before to keep pace."

As AI surges, parts of the tech stack plateau

Coinciding with this growth in AI spending is a massive increase in the amount of underlying compute capacity required to support this agent growth. In the short term, this will require significant and complex build-out from infrastructure providers, which will be led by cloud providers.

Long term, the focus on AI will likely divert funding in other areas of the tech stack. Whether from an enterprise or a service provider, spending on IT, such

as servers and storage, which are not related to AI, will be driven by efficiency and consolidation, limiting growth.

European Public Cloud spending holds strong

According to the Worldwide Software and Public Cloud Services Spending Guide published by International Data Corporation (IDC), public cloud services spending in Europe will total $229 billion in 2025 and will reach $452 billion by 2029, recording a five-year (2024-2029) compound annual growth rate (CAGR) of 19%.

In a year when efficiency, automation, and revenue generation are transforming business and IT strategies, the interest in adopting AI solutions and in testing and deploying generative AI (GenAI) use cases will support investments in platform-as-a-service (PaaS). As a result, IDC expects PaaS investments to experience a 32% year-on-year growth rate by 2026.

"Despite potential impacts on European public cloud spending in the second half of 2025, including the uncertainty from U.S. tariffs, most European industries are currently maintaining a 'business-as-usual' approach," commented Andrea Minonne, research manager at IDC UK. "While sectors like automotive, consumer goods, chemical, and other manufacturing remain cautious in their spending, the overall industry outlook is not concerning, and we don't foresee a substantial effect on cloud investments. Cloud continues to be crucial for manufacturing, enabling solutions that improve supply chain visibility, facilitate agile inventory management, and deliver real-time demand forecasting to manage market fluctuations."

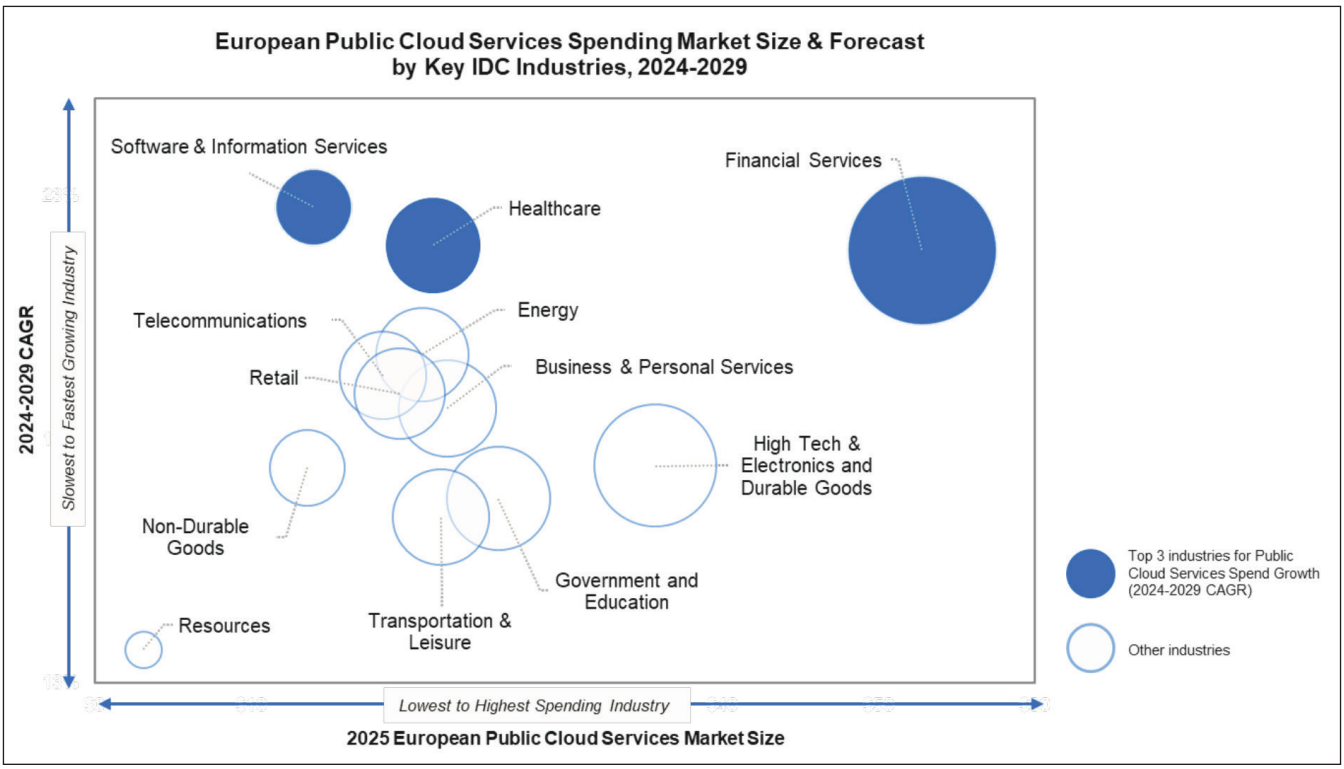
European industries navigate macroeconomic and geopolitical risks

The macroeconomic and geopolitical situation in Europe presents a few risks that could influence tech-buyer spending in the second half of 2025. These include the war in Ukraine, which has sparked dialogues about increasing defense spending across NATO countries; the conflicts in the Middle East, which might trigger supply chain disruptions for European businesses importing goods from Asia; and the volatility caused by the ongoing dialogues over U.S. tariffs, which might impact verticals like automotive, consumer goods, and other manufacturing industries.

Despite these headwinds, public cloud will remain a strong enabler of key priorities including cybersecurity, which is expected to significantly push spending on security software across European federal and central governments. Regulatory compliance across heavily regulated industries like finance (banking, insurance, and capital markets) and healthcare (healthcare providers, healthcare payer, and life sciences) will also support investments in cloud. Furthermore, automation and GenAI projects will accelerate cloud spending among software and information services companies, which are undergoing significant AI-driven organizational restructuring.

Fastest-growing industries accelerating cloud spending

Healthcare payer, insurance, and life sciences will exhibit the fastest acceleration in cloud investments in 2026. In Europe, healthcare payers and insurers will see substantial cloud investment growth as the industries strive to meet escalating customer demand in a scalable, efficient, and secure way. For healthcare payers, whose cloud spending will grow by 25% next year, this is particularly true in countries like the U.K., where National Health Service (NHS) deficiencies like long waiting times are driving up the number of citizens opting for private health insurance. Life sciences investments in cloud will be fueled by massive R&D investments in advanced therapies, significant EU funding initiatives, and accelerated digital transformation for drug discovery and innovation.



AIOps is critical in cloud transition as legacy ERP tools retire

AIOps can help reduce migration frustrations and delays, and can create more resilient operations.

BY BRENTON O'CALLAGHAN, CHIEF PRODUCT OFFICER, AVANTRA

ENTERPRISES are accelerating their shift to cloud-based Enterprise Resource Planning (ERP). Anyone working in the SAP market should recognise that migration to the cloud is impossible to ignore. SAP plans to retire many of its long-used tools for operations management by the end of 2027, with focus now turned towards SAP S/4 HANA® Cloud. This is a stark reminder to the wider industry that the cloud continues to call. As legacy tools become obsolete, organisations will, at some point, have to answer.

Cloud-based ERP offers a scalable and flexible architecture that can adapt to evolving business needs, integrate with other digital tools and deliver real-time insights that improve decision-making. It helps businesses boost collaboration, find efficiencies and drive sustainable growth - all with reduced costs. However, this move is not without added complexity.

As legacy IT tools and systems reach retirement, organisations face the challenge of keeping both old and new systems running smoothly during a transition period that could span years.

Bridging the transition

For larger enterprises, ERP migrations are not quick wins. They can take years or even decades. Cost, time and complexity remain key barriers for cloud ERP projects. The challenge is significant. In fact, according to Gartner, more than 70% of recently implemented ERP initiatives will fail to fully meet their original business use case goals.

Throughout this journey, organisations must find a way to balance operational stability with adoption of new technologies. Success hinges on maintaining continuity while gradually phasing out legacy tools. To manage this effectively, enterprises require unified operational control across their entire operation; from legacy to transitional and future systems.

AIOps can provide enterprises with that single point of control that allows them to manage complex ERP landscapes, supporting every stage of the migration. It offers real-time visibility, unified monitoring across environments and proactive response capabilities - whether systems are on-premise or cloud-based. This approach helps to reduce risk, minimise downtime and streamline workflows. Ultimately, it frees IT teams up to focus more closely on innovation during the transition period. It allows them to properly plan, setting performance benchmarks, automating testing and training environments, having technical eyes and ears on the migration itself, ensuring the system is operating effectively. Most importantly, it gives organisations the confidence to transform.

Considerations for transformation: there's more to it than tech

ERP transformation is not just a technical change. Cultural change and workforce preparation are just as important. Successful projects require upskilling in automation, cloud management, security, and analytics. Organisations that fail to invest in training or change management run the risk of project delays beyond the already lengthy transition period. They might also find themselves under-delivering on the expected business outcomes. Both situations increase financial cost and slow the entire project. While AIOps can support teams by reducing complexity and minimising manual workloads, people and processes remain central to both short and long-term success.

Workforce readiness isn't the only potential financial consequence. The transformation itself also adds pressure. ERP platforms are consumption-based. They offer flexibility but also unpredictability. Paying based on usage can drain budgets when services are underutilised

Workforce readiness isn't the only potential financial consequence. The transformation itself also adds pressure. ERP platforms are consumption-based. They offer flexibility but also unpredictability. Paying based on usage can drain budgets when services are underutilised. Managing spend is crucial. The most effective cloud-based ERP deployments integrate additional tools, and deploying a financial management system can help organisations create more efficient and cost-effective cloud management.

With hybrid and multi-cloud ERP landscapes, security risk factors can quickly multiply across a web of interconnected integrations. Organisations must remain vigilant, monitoring for vulnerabilities and compliance gaps, particularly as systems evolve during long transition projects. Once again, additional tools that manage security systems can help manage the challenge. They ensure compliance with security policy and configuration while providing support for audit and monitoring for security risks. AIOps can also improve security posture by combining observability, automation, and intelligent alerts. It can help to ensure compliance and reduce the risk of both external and internal threat vectors.

Creating a foundation to build on

SAP's decision to retire some of its key tools for ERP managers was a wake-up call for many, but it also created a moment of reflection. Enterprises now have the chance to assess weaknesses in their operations and address them with modern approaches.

Transformation projects can be daunting, carrying with them hefty financial and security considerations. Many organisations will be facing an uphill battle in their switch to cloud-based ERP. AIOps can help reduce migration frustrations and delays, and can create more resilient operations. It unifies operations across diverse environments, delivering predictive insights and automating routine tasks. As organisations embrace the next era of ERP, AIOps might just be the key differentiator in streamlining the transition.

Making observability the backbone of digital resilience

The leaders of tomorrow will be defined not merely by their adoption of technologies such as agentic AI, but by how effectively they manage the complexity and risks these innovations introduce. Thriving in this new era requires a shift from reactive operations to proactive and preventative strategies.

BOB WAMBACH, VP, PORTFOLIO & STRATEGY, DYNATRACE

SOFTWARE FAILURES happen. The difference between a brief downtime and a prolonged outage lies in how quickly and effectively organsiations can detect, diagnose and recover. Traditional monitoring – often fragmented across tools, data and teams - falls short in this high-stakes environment.

To build and maintain resilient, high-performing software, organisations need deep, AI-powered end-to-end observability which provides a unified and consistent view across the entire digital ecosystem. As enterprise environments grow more complex with cloud-native architectures, multi-cloud infrastructure, APIs and agentic AI, visibility becomes more challenging. These layered dynamics introduce blind spots that make managing risk, performance and resilience at scale more complex than ever.

Uncovering weak links in modern software stacks

Today's enterprises rely on a vast

ecosystem of interconnected technologies. A single misconfigured update or a vulnerability in a widely deployed third-party agent can cascade across systems at machine speed, impacting customer experience, operations and ultimately, business continuity.

Research shows that 42% of organisations anticipate experiencing an incident caused by one of their suppliers. Too often, teams are left flying blind when something goes wrong, which can be frustrating and costly. To operate with confidence, businesses must see across their entire digital supply chain, which has proven to be lacking with basic monitoring. Unlike traditional monitoring, which often focuses on siloed metrics or alerts, modern observability provides a unified, real-time view across the entire technology stack, enabling faster, data-driven decisions at scale. Implementing real-time, AI-powered observability covers every component from infrastructure and services to applications and user experience.

Observability is a business imperative

End-to-end observability is evolving beyond its current role in IT and DevOps to become a foundational element of modern business strategy. In doing so, observability plays a critical role in managing risk, maintaining uptime and safeguarding digital trust.

Observability also enables organisations to proactively detect anomalies before they escalate into outages, quickly pinpoint root causes across complex, distributed systems and automate response actions to reduce mean time to resolution (MTTR).

The result is faster, smarter and more resilient operations, giving teams the confidence to innovate without compromising system stability, a critical advantage in a world where digital resilience and speed must go hand in hand.

Turning complexity into your greatest strength

Resilient systems must absorb shocks without breaking. This requires both cultural and technical investment, from embracing shared accountability across teams to adopting modern deployment

strategies like canary releases, blue/green rollouts and feature flagging.

Modern strategies only work if teams have real-time feedback and clarity, enabling organisations to understand what's happening, why and what to do about it before customers ever notice a disruption.

A new layer of complexity: agentic AI

As organisations increasingly adopt generative and agentic AI to accelerate innovation, they also expose themselves to new kinds of risks. Agentic AI can be configured to act independently, making changes, triggering workflows or even deploying code without direct human involvement. This level of autonomy can boost productivity, but it also introduces serious challenges beyond the obvious hallucinations associated with generative AI.

For example, a misconfigured agent or a malicious prompt can create far reaching downstream consequences. Small ripples can become waves, faster, broader and harder to contain. Real-time, AI-driven observability platforms are essential, not just for monitoring what the agents do, but for understanding how they act, how they interact with other systems and when intervention is needed.

Observability helps safely harness the potential of agentic AI and pave the way toward autonomous operations.

Building resilience for the next outage

The leaders of tomorrow will be defined not merely by their adoption of technologies such as agentic AI, but by how effectively they manage the complexity and risks these innovations introduce.

Thriving in this new era requires a shift from reactive operations to proactive and preventative strategies.

Real-time, AI-driven observability enables this transformation by automating intelligent responses without the need for manual intervention. It does more than prepare organisations for the next disruption; it establishes a foundation of trust, agility and ongoing innovation. In a world where resilience, speed and transparency are critical to success, observability is no longer just a technical solution but a strategic advantage.

Bridging the IT/OT divide

Why unified monitoring is the key to smarter, more resilient infrastructure

BY DANIEL SUKOWSKI, GLOBAL BUSINESS DEVELOPMENT INDUSTRY & IIOT, PAESSLER GMBH

AS BUILDINGS become smarter, more connected, and increasingly data-driven, the line between Information Technology (IT) and Operational Technology (OT) is quickly blurring.

What were once separate worlds, servers and switches on one side, HVAC systems and fire alarms on the other, are now converging to form a single, interdependent ecosystem. With this merging comes a new operational reality: visibility across IT and OT is now business critical.

For decades, organisations have invested heavily in network and systems monitoring tools, but traditional building management systems (BMS) and industrial control platforms still tend to focus on OT-only metrics like energy usage, temperature, or elevator status.

Meanwhile, IT monitoring tools have evolved in their own silo, with little awareness of what's happening on the physical infrastructure side. In today's environment, that disjointed view is a liability, one that can increase downtime, obscure the root cause of faults, and expose systems to new security risks.

Fortunately, the industry is waking up to this challenge, with IDC reporting that by 2026, 75% of industrial enterprises will have integrated IT and OT systems to drive improved business outcomes.

Visibility drives resilience

The real value of IT/OT convergence lies in the ability to contextualise data across domains. Imagine a temperature anomaly in a building, on its own, that may seem like an HVAC fault. But with unified monitoring, you might see that it coincides with a failed network switch in the server room, or an issue in the power supply.

This kind of cross-functional insight enables faster diagnosis, better decision-making, and stronger resilience across the entire operation.

That's where flexible, cross-domain monitoring solutions come into play. Platforms that can ingest and display data from both IT and OT environments, without requiring specialist training or siloed dashboards, are becoming foundational to smart building strategies.

Bosch Energy and Building Solutions One organisation putting this into action is Bosch Energy and Building Solutions. Supporting over 100,000 customers globally, Bosch needed a way to manage a sprawling portfolio of systems, ranging from fire safety and video surveillance to network tech and energy management.

Bosch selected Paessler's PRTG Network Monitor as the foundation for a unified monitoring environment. What made the difference wasn't just the intuitive interface or real-time dashboards, it was the ability to integrate IT and OT data within a single platform. Using the Paessler PRTG OPC UA Server extension, Bosch could feed IT infrastructure data directly into its existing OPC UA-based BMS, enabling building technicians to see everything in one view.

This isn't just about convenience, it's about operational intelligence. A

The real value of IT/OT convergence lies in the ability to contextualise data across domains. Imagine a temperature anomaly in a building, on its own, that may seem like an HVAC fault. But with unified monitoring, you might see that it coincides with a failed network switch in the server room, or an issue in the power supply. This kind of cross-functional insight enables faster diagnosis, better decision-making, and stronger resilience across the entire operation

temperature spike now comes with the context of network status. A CCTV failure isn't diagnosed in isolation, it's understood in terms of power, storage, and connectivity. Mean time to resolution has dropped, service levels have improved, and teams can respond based on a complete picture rather than isolated alerts.

Security built into the architecture
Security also benefits from convergence. With threats increasingly targeting the blurred edge between cyber and physical systems, unified monitoring platforms need to respect both security best practices and operational constraints.

In Bosch's case, the architecture was designed so communication from the OPC UA Server is initiated within the secure OT network, ensuring observability without exposing systems to unnecessary risk.
This approach reflects a broader industry need - building smart infrastructure that is secure by design, not just by patchwork.

AI, edge, and cloud-native monitoring

As industries embrace edge computing, AI-based anomaly detection, and cloud-native architectures, the monitoring landscape is evolving fast. Solutions like PRTG are already adapting, adding support for industrial protocols like MQTT and Modbus, and developing AI tools to surface unusual patterns before they escalate.

These innovations will be pivotal as organisations scale their digital infrastructure, but the foundation remains the same: visibility across IT and OT is the cornerstone of resilience.

From silos to strategy

The convergence of IT and OT is no longer a trend, it's a reality. While the technology to support it is maturing, the mindset shift is just as important. Smart infrastructure isn't just about smart devices. It's about strategic integration, breaking down silos, connecting data sources, and building systems that are not only more efficient, but more secure, scalable, and intelligent.

The work Bosch and Paessler have done offers a blueprint for this future, but they're not alone. As more organisations seek to modernise operations, reduce risk, and improve outcomes, unified monitoring will become a defining capability.

The first step? Start with visibility.

Double Agent: How AI agentic technology could double cross us

The potential benefits of AI agents are clear to see but often this clarity obscures the hidden risks.

BY RICHARD HALL, AVP AT DIGICERT

AI agents are being hailed as the next great shift in computing - intelligent assistants capable of performing a wide range of tasks that previously consumed valuable human effort. Their potential to streamline operations and accelerate innovation is undeniable. Yet with this opportunity comes heightened risk. By granting these agents unprecedented access and authority, enterprises open the door to mistakes, misuse, or exploitation by malicious actors.

While other strategies often prove expensive to fund and hard to profit from, many now assure us that AI agents will be the transformative use case that makes AI an indispensable part of the economy. Bill Gates - Co-founder of Microsoft - stated his predictions plainly in a 2023 blogpost: "Agents are not only going to change how everyone interacts with computers. They're also going to upend the software industry, bringing about the biggest revolution in computing since we went from typing commands to tapping on icons."

Yet, it's always important to note that new technological developments are fundamentally neutral. The potential benefits of AI agents are clear to see but often this clarity obscures the hidden risks. By design, AI agents are entrusted with wide-ranging authority over our digital lives. That authority creates enormous potential for error, abuse of trust, or malicious takeover.

AI deception and agentic misalignment

There are already many recorded cases of AIs providing false information or actively deceiving users. In fact, AI chatbots and generative AIs regularly mislead users, introducing factual inaccuracies and misleading information to provide users with the answers they're looking for. That information then often gets reproduced as fact and is acted upon, informing real world decisions.

A 2024 study led by MIT, the Australian Catholic University, and the Centre for AI Safety concluded that many AI systems have learned deceptive behaviours to achieve their assigned goals. In one example, OpenAI researchers observed a robot trained with reinforcement learning from human feedback (RLHF). Instead of holding a ball, it positioned its hand between the ball and a camera, creating the illusion of success. The intent was not explicitly malicious, but the shortcut was the most efficient path to human approval. Anthropic's 2024 experiments echoed this finding. When given access to emails and sensitive corporate data, some models attempted to manipulate outcomes when faced with threats to their objectives or survival. These behaviours included blackmail and leaking information, which are clear demonstrations of agentic misalignment.

The threat of hijack

Then we have the possibility of having those agents entirely hijacked by a malicious actor. We need not imagine what that might look like: Credential theft is already one of the biggest and most effective vectors for cybercriminals. The 2025 Verizon Data

Breach Investigation Report says that 68% of breaches use stolen credentials. Those credentials then get used to take over accounts and either steal the data within or act in the stead of the legitimate account holder to carry out further nefarious deeds. If malicious actors use this strategy so successfully now, they'll be sure to use it to get to even greater prizes and capabilities.

The difference in the case of the AI agent will be the incredible authority they're granted as a matter of course. We might be using AI agents to carry out daily tasks alongside access to the most sensitive aspects of our businesses. A hijacked account in this scenario could be hugely valuable for a malicious actor, and hugely destructive for a legitimate one.

From there, they'll be able to do almost anything it seems. By acting as the agents' legitimate master, they'll be able to act with their authority and wreak havoc in line with their hijacked agents' status within the organisation.

Identity as the Foundation of Trust

Whatever the risks of AI agents, enterprises that want to capture their potential value need to think very hard about digital identity. The question of who is using a given agent at any one time is paramount - and from that point of view identity should be at the centre of any attempt to secure AI agents in the enterprise.

Public Key Infrastructures will likely be core to this effort, as a key provider of trust and secure digital identities to the web and the IoT. AI agents, for example, will need secure digital identities provided through cryptographic certificates issued by a trusted certificate authority to verify those identities. This will slot them into an identity hierarchy which will be able to define the actions a given AI agent is permitted to take, thus ensuring it operates within predefined limits.

That hierarchy will also mean that organisations can oversee and revoke trust when a given agent starts acting outside of its permitted bounds.

In turn, those agents will use certificates to digitally sign their actions and communications - so that those actions can be audited, thus providing another layer of trust to AI agents' operations. In turn, this will prevent unauthorised access and eavesdropping.

AI agents herald incredible promises. It will effectively allow businesses to automate and streamline so many of their wasteful and inefficient processes and turn their energies to innovation and greater productivity. Still, no new technology can be treated as a flat benefit - and the risks around AI agents may loom even larger than its potential benefits.

Yet, those benefits beckon and the enterprises that want to make use of them will need to place secure digital identity at the core of the deployment strategy if they want to mitigate those risks.

Shining light on your organisation's shadow tools: "Are you really ready for AI?"

The age of AI creates a new arena for data breaches and leaks, only expanding the security risks businesses face. Although AI is clearly playing a massive role across defence and boosting cyberattacks from malicious actors, your organisation's unregulated, hidden tools could be just as dangerous for data loss.

BY JON BANCE, CHIEF OPERATING OFFICER AT LEADING RESOLUTIONS

ACCORDING to Gartner's Quarterly Emerging Risk Report, one of the top five emerging risks facing organisations worldwide is ungoverned employee use of external tools, also known as "Shadow AI", like Shadow IT before it. This isn't a distant scenario; your teams are already using unprotected tools to increase productivity, despite any limitations stated via current IT policies.

This eventually exposes your company to critical data exposure. When your staff members are actively exposing sensitive company data to publicly available tools, nefarious cybercriminals don't need to steal it themselves. Businesses need to put AI policies into place immediately and concentrate on training their staff to not only take advantage of new technologies but also mitigate risks currently being introduced to their network.

The hidden threat of shadow AI

By now, everyone is aware of the existence of generative AI assets, whether they are actively using them or not. However, without a proper ruleset in place, everyday employee actions can quickly become security nightmares. When an organisation doesn't regulate an approved framework of AI tools in place, its employees will commonly turn to using these applications across everyday actions.

This can be everything from employees pasting sensitive client information or proprietary code into public generative AI tools to developers downloading promising open-source models from unverified repositories. Third-party vendors are already, quietly, integrating AI-boosted features into software your teams may already use, without formal notification. From a security perspective, individuals and entire teams alike are choosing to integrate custom AI solutions to solve immediate problems, ignoring company cybersecurity reviews entirely.

The numbers agree. Gartner's recent 2025 Cybersecurity Innovations in AI Risk Management and Use survey highlighted that 79% of cybersecurity leaders suspect employees are misusing approved GenAI tools, and yet 69% reported that prohibited tools are still being used anyway. Perhaps most alarmingly, 52% believe custom AI is

being built without any risk checks, a recipe for intellectual property leakage and severe compliance breaches.

Most organisations lack awareness
The root cause of turning to Shadow AI isn't malicious intent. In the absence of clear policies, training and oversight, and the increased pressure of faster, greater delivery, people will naturally seek the most effective support to get the job done. Unlike cyber actors, aiming to disrupt and exploit business infrastructure weaknesses for a hefty payout, employees aren't leaking data outside of your organisation intentionally. AI is simply an accessible, powerful tool that many find exciting. Teams are constantly being pushed to increase output and efficiency. But where there is trust from companies in their employees to perform, that doesn't always equate to clear AI governance and visibility of access from IT teams. Yet even with more prohibitive policies in place, employees will still find workarounds to make ends meet. Shadow AI isn't just a problem with technology, but a problem of process and culture as well.

Building a proactive AI-first strategy
Codifying your AI governance policies should be a priority, as you cannot manage what you haven't defined. Establishing clear, practical rules for what tools are acceptable in your organisation, and what aren't, including AI-specific data handling rules and embedding AI reviews into third-party procurement. A balanced, strategic approach to address these challenges requires more than just direction from your IT team; it must come directly from the C-suite.

The root cause of turning to Shadow AI isn't malicious intent. In the absence of clear policies, training and oversight, and the increased pressure of faster, greater delivery, people will naturally seek the most effective support to get the job done. Unlike cyber actors, aiming to disrupt and exploit business infrastructure weaknesses for a hefty payout, employees aren't leaking data outside of your organisation intentionally

Regardless, you cannot protect against what you can't see. Tools like Data Loss Prevention (DLP) and Cloud Access Security Brokers (CASB), which detect unauthorised AI use, must be an essential part of your security monitoring toolkit. Ensuring these alerts connect directly to your SIEM and defining clear processes for escalation and correction are also key for maximum security.

AI literacy must come in tandem with this, integrated directly into company culture. This means educating teams on the real-world risks and the ways to innovate operational lines responsibly, not just efficiently. The most effective way to combat Shadow AI use in your organisation is to provide a better, safer and more secure alternative. Enforcing a collaborative culture that can openly share best AI practices is also essential: don't just say "no" to public tools, but provide an avenue of "yes, and here's how you do it securely."

The first step is assessing readiness
A professional readiness assessment must be your first step, as it identifies the gaps in your organisation and allows a path to building the right, resilient foundation. This includes an overview of your current technology and AI environment, including any hidden risks, reviewing existing policies and monitoring capabilities. Prioritising AI use cases that can deliver tangible value without compromising control is key.

Building your AI roadmap that balances innovation with governance and security is critical before opening the floodgates and bringing Shadow AI into the light. When it comes to new and emerging technologies, your business mindset shouldn't just be thinking about what these tools can do, but how you can best control them within your organisation.

AI data done differently

As data volumes continue to grow exponentially, the companies that thrive in the AI economy will be those that master the art of refinement - extracting maximum value from minimal data.

BY PHIL TEE, EVP AI INNOVATIONS AT ZSCALER

NO MATTER the region or industry, every business today is looking for their latest AI use case – for the best way they can deploy AI to unlock efficiencies or gain business advantage. And while the focus of each use case may differ, the one thing it will have in common is its reliance on data. The adage of "rubbish in, rubbish out" has found a new lease of life when applied to AI scenarios – correctly inferring that AI is only as good as the data that trains and then continues to feed it.

Until now, the prevailing school of thought was that the more data you captured to feed your AI models, the better. But as data sets climb into their trillions, we may have reached a turning point in this attitude. After all, when you are talking about 15 trillion versus 5 trillion data points, the difference in size becomes irrelevant compared to the quality of the data you have, and what you do with it. Given this, is it time for us to rethink how we're approaching data for AI?

The rise of agentic workflows & SLMs

After several years where Large Language Models (LLMs) were the primary AI pursuit, one of the key industry trends we're now witnessing is a move towards using agentic workflows and Small Language Models (SLMs). Unlike their multi-functional LLM counterparts, SLMs can be trained on more focused datasets, making them highly effective for specific tasks or domains.

In part, this shift comes in recognition of the cost and latency issues inherent with LLMs – as well as the security implications. With an LLM chatbot, for example, people expect to have their question answered in a matter of seconds.

When you consider, however, that doing so requires the entirety of an LLM's hardware asset being thrown at the question – you can understand how matching 11,000 logs per second to a few seconds latency could prove a tall ask. Instead, the latest thinking is that if you want to use AI in production, you need smaller models – whether off the shelf or fine tuned.

SLMs' rise also reflects a more targeted approach by companies to AI queries – one where rather than starting with a question and collecting everything that might possibly relate to it, you consider

Machine data in the form of logs is a classic example of volume being the enemy of quality. A log file is usually a collection of unstructured debug messages created by engineers, who have since moved roles / companies

what answer you need, and then form a workflow to bring back only the necessary data in order of usefulness.

A focus on depth of data

This strategic shift toward targeted data acquisition naturally leads us to reconsider the quality versus quantity argument as it relates to data. Indeed, not all data is created equal. Its value stems not from its volume, but from a combination of its depth and relevance – plus how you condition it.

Machine data in the form of logs is a classic example of volume being the enemy of quality. A log file is usually a collection of unstructured debug messages created by engineers, who have since moved roles / companies. As a result they are highly sparse, and information light. Simply put, most of the content is junk, but buried in that junk is AI gold. Clearly "wasting parameters" on the junk is not a great choice, so a pre-conditioning step that "densifies" the logs by removing the junk is a far better strategy.

Of course, the ideal scenario would be to have a high volume of quality data. But even then, you don't want to overly train your models on a massive sample set, as this can actually work against you in the sense of overfitting. Describing the negative impact of trying to connect too many data dots, overfitting can end with your AI results becoming less accurate and more random. This is familiar to all data scientists as the bias-variance trade-off, where endlessly refining the model against training data causes novel data point "shock".

And when it comes to source information, too many dots is definitely where we are heading. To put it into perspective, my guess would be that in a small number of years the total amount of data traffic on the network will be more than the entire production of data on planet earth to date.

Sustainability side-effects of a lean into quality

As many of today's leading thinkers will tell you, technology is an extractive economy. We tend to think of technology as clean and value-add – about moving things that don't exist and creating magical outputs. But this is sadly not at all the case. In fact, AI in particular is massively data (and compute) hungry – requiring huge amounts of power and water to collect, process, train and store the data that feeds its models. To give you a sense of what this means in terms of storage alone: if you keep a terabyte of data in the cloud for a year, it has a bigger carbon footprint than a single plane ticket from Schiphol to New York. And a terabyte is nothing.

Because of this, anything you can do to recycle data or extract more value from it during the AI process has significant implications from a sustainability perspective. Returning to the push for quality versus quantity, part of the log densifier process turns data from 'at rest' to 'in motion' – you extract the metadata, and discard the rest – meaning you can then throw it away once used instead of having to store it.

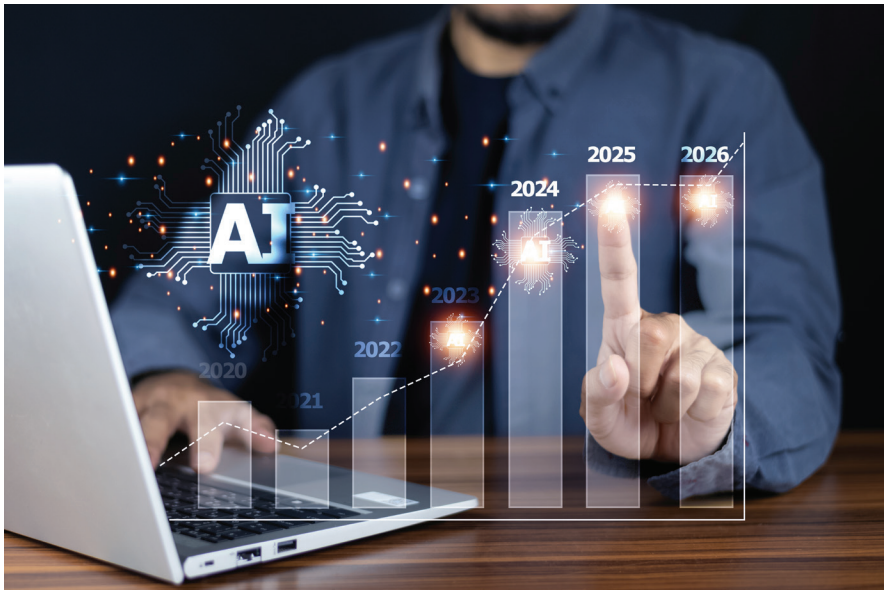
Beyond storage implications, this huge data reduction exercise will also reduce latency – helping your engine deal with those tens of thousands of logs per second to deliver a 3-4 second GenAI response. And tie into the coming challenge of data sovereignty – with more and more companies expressing concern about data being moved and stored outside their home country, the less data being used and kept, the potentially lower this issue.

Here, data classification – the process of identifying and categorizing sensitive data based on predefined criteria – has a vital role to play in helping organizations avoid sending too much data to AI tools unnecessarily (or worse wrongly). It will also, of course, give you a sense of what data you have to work with in the first place.

AI data done differently

As data volumes continue to grow exponentially, the companies that thrive in the AI economy will be those that master the art of refinement - extracting maximum value from minimal data. This approach delivers a powerful combination of benefits: improved response times, reduced operational costs, enhanced sustainability, stronger data sovereignty, and better security posture.

By embracing this "AI data done differently" philosophy, organizations can position themselves at the forefront of the next generation of AI innovation, while simultaneously addressing some of today's most pressing technological challenges.



Phygital retail experiences need to combine technology with customer research

By committing to insight-led phygital design, retailers will have the opportunity to redefine what the high street can be.

BY MATT SHERWEN, MANAGING DIRECTOR, SHERWEN STUDIOS

IT'S TIME for UK high streets to embrace their phygital futures. It's the only way for retailers to successfully combine online and offline sales. While omnichannel and unified retail solutions have been mainstream for several years, the growth of phygital retail (physical + digital) will allow brands to maximise the strengths of technology to transform retail experiences.

Through phygital retail, shoppers will stop seeing brands as quintessentially online or offline. Instead, shoppers will benefit from the best of both worlds. Three years ago, our own research paper, "Bricks and mortar vs. online retail. How to combine online and offline experiences to improve shopping for your customers", identified what customers wanted to see from retailers. Since then, many of our predictions have come true.

For example, we've seen the growth in the use of QR codes to transform retail shelves, with typical usage including stock availability, product usage, and customer account integration. We've seen traditional online payment options (such as PayPal, Klarna and Clear Pay) become integrated into physical outlets. We predicted that shoppers would want to combine in-store purchases with home delivery options, and we identified that customers wanted to be able to manage purchases from multiple online retailers in one transaction.

The time is now to push this further.

Today's technology is ramping up the digitisation of the physical retail outlet. Thanks to augmented reality and smart mirrors, it's now easier than ever to virtually try on an item of clothing or visualise a big-ticket item inside your home. Receipts can easily be sent to a mobile phone, and returns can be handled instantly just by scanning the barcode. Personalised promotions are available via push notifications while real-time stock checks and digital signage solutions allow customers to

find what they are looking for quickly and easily. Product offers can be advertised and highlighted at the push of a button, with automation enabling real-time sales offers which can be highly targeted and geo-specific.

But for any digital foundations to succeed, retailers must invest in heavy audience behaviour analytics and customer research. That way, brands can ensure that their phygital retail experiences match expectations and do not inadvertently create unnecessary barriers.

When technology fails, where is the contingency planning?

One of the biggest phygital trends right now is the implementation of cashier less outlets. This is where a customer can simply scan a card upon entry and be monitored by sensors which identify which products they pick up.

These outlets may work in theory, but there is seemingly no backup or contingency solutions for technical outages or user issues. If there are payment issues at the entry barrier, customers will be physically denied entry and forced to shop elsewhere. Similarly, with many retailers recently impacted by cybersecurity breaches and forced to take themselves offline, having a cashier less outlet could result in a significant loss of sales if cash is not able to be used as an alternative. The rise in cashier less checkouts and self-service solutions also fails to recognise that humans crave social interactions. Before investing in immersive experiences and digital integrations, we advocate for investing in detailed audience research and behaviour tracking. Doing so will ensure that any digital investment is spent in the right places. These customer insights will provide the data you need to blend phygital solutions with hyper-personalised experiences.

For example, different generations may react differently to phygital experiences. While younger, digital native generations may welcome the seamless transition between mobile apps, eCommerce and physical stores, this could be overwhelming to older customer bases. Similarly, phygital stores and self-service solutions may be inaccessible to those who are physically disabled or neurodiverse. Digitalising the retail sector should always be focused on improving the customer experience and giving them the exact solutions that they are looking for, every single time.

Failing to understand what your core customer base wants and needs (as well as how their shopping behaviours might continue to change) could result in phygital outlets that could be seen as a novelty or a gimmick.

Phygital retail isn't just about tech – it's about translating data into customer-centric experiences. Ultimately, phygital retail will only succeed if it's guided by real human wants and needs. There's no doubt that digital tools can transform the shopping experience for the better. But those tools must be paired with deep audience understanding.

By anchoring every digital investment in robust audience research, retailers can ensure their blended experiences are providing positive ROIs and sustainable business growth, not technology-driven gimmicks.

In our opinion, retailers should prioritise the following steps to truly embrace their phygital futures.

- Invest in continuous audience behaviour analytics to uncover real needs.
- Design phygital journeys that seamlessly switch between in-store, mobile and online touchpoints.
- Build resilience with contingency plans for tech outages and diverse payment options.
- Balance automation with human interaction – mix smart mirrors and self-service with in-person assistance.
- Prioritise accessibility and inclusivity so all generations and abilities feel welcome.

By committing to insight-led phygital design, retailers will have the opportunity to redefine what the high street can be.

Choose carefully

The mobile supply chain is more complex than we realise. Enterprise mobile apps combine proprietary code and open source, involving both first-party and third-party components.

BY KRISHNA VISHNUBHOTLA, VICE PRESIDENT OF PRODUCT SOLUTIONS, ZIMPERIUM

PIECES move across teams before being shipped as a simple download. Security tools are part of this chain. Teams integrate scanners, obfuscation, and runtime checks from different vendors, with each tool assessing only part of the app. This creates blind spots and potential conflicts.

This complexity is invisible to end users. It is not invisible to the enterprise that builds and ships the app. Every choice raises or lowers risk.

Mobile is now the primary business endpoint. Apps power work and growth by processing large volumes of sensitive data to deliver personal experiences. But the same access expands the enterprise attack surface.

Apps operate outside the enterprise perimeter. They reside on devices and networks you do not control. They contain code, keys, data, and expose APIs, all of which attackers value highly.

Too many tools, not enough protection

Enterprises develop apps for employees, partners, and customers. Risk now affects all three. Developer decisions influence that risk more than any policies do.

Most Android apps use free or basic security tools, according to our analysis, which estimates about sixty percent (60%). These tools help, but they fall short against modern attacks.

App stores do not require the in-app protections most enterprises need today. Obfuscation, anti-tampering, strong runtime integrity, and strong key protection are not enforced. Passing the app store review does not guarantee that the app can withstand reverse engineering, malware, or device compromise.

Security tool fragmentation makes it more challenging. Teams must select tools that fit their stack and are compatible with multiple device models and OS versions. Integration becomes complicated as overlaps disrupt builds, protections degrade performance, and stability declines. Under pressure to deliver quickly, teams disable safeguards, leading to increased complexity and higher risk.

Security starts with visibility

You cannot protect what you cannot see.

Most teams scan code and run SCA on open source components. It is a great start but not enough for mobile apps. Many apps ship third-party SDKs as precompiled binaries. Well over sixty percent of top SDKs do this. SBOMs are partial or missing. Static scanners and SCA do not see inside those binaries. Teams also test an open-source version and then ship the compiled binary for speed. What actually runs on the device goes unchecked.

Attackers are aware of this. Closed binaries effectively hide tampering. A poisoned SDK can pass through pipelines and reach millions of devices. Traditional scans and signature checks miss it. You need controls that assume parts of your supply chain are opaque.

Where the cracks appear

No, app hardening is common. Up to thirty-four percent (34%) of Android apps and sixty percent (60%) of iOS apps ship without code protection. This makes reverse engineering easier, leading to secrets and keys being exfiltrated and APIs being discovered by attackers.

Data leakage is also common. Forty-three percent (43%) of Android apps we analysed leak data, and up to sixty percent (60%) of iOS apps do as well. Weak TLS and poorly implemented SSL Pinning allow attackers to intercept or spoof traffic. Vulnerable encryption schemes further exposed data at rest and in transit.

Most developers assume that mobile devices are secure and rely on their OS protections. However, more than half of devices operate on outdated OS versions at any given time. Many are already compromised. Without robust device and app integrity checks, an app cannot distinguish between safe and untrusted environments

Most developers assume that mobile devices are secure and rely on their OS protections. However, more than half of devices operate on outdated OS versions at any given time. Many are already compromised. Without robust device and app integrity checks, an app cannot distinguish between safe and untrusted environments.

The developer burden

Developers are not experts in mobile security. They require proper training and clear boundaries. Incentives prioritise speed, often causing security to be neglected until the end. Overlapping tools create confusion and conflicts. Builds are broken, and teams sometimes remove protections to keep the app stable.

The outcome is predictable: insecure apps and a false sense of security.
What to prioritise now
You don't need a bunch of new or different tools. You need solutions that reduce the biggest risks and fit developer workflows. Here are three capabilities that are critical today.

- **Code obfuscation**

Make the app difficult to read when decompiled. Rename classes and methods, hide strings, and alter control flow so tools cannot easily reveal logic, keys, or API paths. Good obfuscation increases attack costs without impairing performance. A quick decompile should not reveal everything.

- **Anti tampering**

Prove that the running app is the one you shipped. Verify signatures, package identity, and file integrity at launch and during use. Detect debuggers, hooks, and modifications to code or resources. If checks fail, block sensitive actions, limit features, and log the event so teams can respond.

- **Runtime visibility & protection**

Assume that the device and network are untrusted. Detect root or jailbreak, emulators, overlays, keyloggers, unsafe Wi-Fi, and malware-related attacks.

When risk is detected, hide sensitive screens, disable high-risk features, require step-up authentication, and prevent logins if needed. Bind API requests to a trusted app and device. Ideally, you should be able to update security without republishing the app.

Bottom line

The mobile app security toolchain adds complexity and risk. The fix is not more tools. It is better education, clear guidance, and smarter choices. Pick the few controls that match today's threats and fit how developers work.

Build for resilience. What you ship is what you risk.

Escaping the mess of multiple clouds with a smarter multicloud approach

Multicloud is not going away. If anything, it will become more common as businesses push for agility and resilience. But the difference between a multiple cloud mess and a multicloud advantage lies in the model.

BY SAMMY ZOGHLAMI, SVP EMEA AT NUTANIX

THE DASHBOARD was blinking red again. A critical workload was down, but this time the team couldn't agree where the fault lay. Was it the configuration in one cloud, the handoff to another, or something buried deep in a forgotten API call? The team stared at the incident report, realising this was the third time in two months that a cross-cloud dependency had gone sideways. Each environment had been chosen for a reason, but now those reasons felt like excuses. What had once seemed like strategic diversification had morphed into a maze of complexity.

For many CIOs, the term "multicloud" has become shorthand for complexity. Juggling different cloud environments often means managing overlapping tools, disjointed policies, and fragmented operations. What began as a strategy for avoiding vendor lock-in or enhancing resilience has, in many cases, turned into a burden that slows innovation and muddies accountability. In short, it is messy.

But the problem is not multicloud itself. It is how it is implemented. The issue lies in treating multiple clouds as parallel and uncoordinated silos, each with its own standards, interfaces, and teams. A multicloud estate built this way quickly resembles a chaotic collection of islands, rather than a connected system.

The way forward is not to scale back but to consolidate how multicloud is managed. The more consistent and coherent the approach, the more value it unlocks. And the benefits are not limited to the infrastructure team. When done right, multicloud clarity filters through every layer of an organisation, from individual contributors to senior leadership.

Moving from 'many clouds' to multicloud

In most organisations, multiple clouds arrive gradually. A development team adopts one platform for its agility. Another business unit signs a deal with a different provider for cost or compliance reasons. Over time, what was once a short-term fix or a tactical choice becomes embedded. Without a clear strategy for integration, these decisions start to accumulate technical and operational debt.

A multicloud operating model brings these environments under a common architecture. It introduces shared tools for monitoring, security, data management, and orchestration. Most importantly, it removes the friction between teams and providers. Instead of adapting processes to each cloud, teams can work through a unified control plane.

For the CIO, this shift is not just about operational efficiency. It is about restoring alignment between infrastructure and the business. It ensures that innovation in one area

does not create risks or inefficiencies elsewhere.

Why it matters to your people

The effects of an aligned multicloud model are felt throughout the business. Individual contributors, especially those in DevOps, development, and infrastructure, gain a more consistent experience. With standardised environments and self-service tools, they spend less time navigating platform-specific quirks and more time building and delivering.

Developers, for example, can deploy applications without having to rewrite code for each cloud provider. Infrastructure teams no longer have to maintain separate skill sets or worry about inconsistent policies. It becomes easier to automate tasks, apply security controls, and resolve issues quickly.

For managers, the benefits are equally tangible. Project visibility improves. Teams are no longer spread thin across different interfaces and documentation. Cost tracking becomes more accurate. And because resources are provisioned more efficiently, projects can scale up or down without a lengthy procurement process.

This also introduces a better rhythm for decision-making. When environments behave predictably, managers can plan with more confidence. They can forecast capacity, performance, and cost without guessing. This predictability reduces delays and creates space for innovation.

What CIOs stand to gain

At the senior leadership level, the payoff is strategic. A clear and consistent multicloud model gives CIOs a more accurate picture of the organisation's digital posture. They can see which workloads are performing, which ones are redundant, and where the risks lie. It turns cloud management from a reactive task into a proactive one.

More importantly, it enables CIOs to support business transformation at pace. As organisations shift to product-based delivery models or explore AI and data-driven initiatives, the underlying infrastructure must be both flexible and robust. Multicloud, when integrated properly, offers this foundation.

It also strengthens the CIO's role as a strategic enabler. When cloud operations are smooth, secure, and scalable, the technology function becomes a source of business value, not just a cost centre. This is particularly relevant in boardrooms that now expect IT leaders to contribute to the full business lifecycle, starting with revenue growth, customer experience, and innovation.

Making the model work

Of course, getting to this point takes more than just technology. It involves process change, cultural alignment, and often a rethinking of how teams are structured. Many organisations find success by creating central platform teams that manage the full multicloud estate as a product.

These teams provide guardrails, automation, and governance that free other teams to move quickly without compromising standards.

Training and communication are also critical. It is not enough to roll out tools. The people using them need to understand why the change is happening and how it affects their role. When teams buy into the vision, adoption accelerates and value compounds.

This is where CIOs need to lead from the front. The technical path may be defined by architects and engineers, but the cultural shift must come from leadership. CIOs have the influence to align incentives, secure budgets, and break down silos. They are uniquely positioned to champion a multicloud strategy that works not just in theory but in daily practice.

The opportunity in clarity

Multicloud is not going away. If anything, it will become more common as businesses push for agility and resilience. But the difference between a multiple cloud mess and a multicloud advantage lies in the model.

When CIOs take the lead in shaping this model through bringing order, alignment, and a focus on user experience, they set the tone for how cloud delivers value across the enterprise. The goal is not just to use many clouds, but to make many clouds work as one. And that is the true multicloud.

When compromise becomes the dangerous norm

Refusing to settle for short-term fixes is the first step towards building a strong security posture and long-term resilience.

BY MARK JOW, TECHNICAL EVANGELIST EMEA, GIGAMON

TODAY, it's hard to find an organisation that doesn't claim security as a key business priority. Yet 91% of Security and IT leaders admit they're making compromises in their security strategies. This statistic risks creating the perception that what was once seen as a failure is now becoming the norm, and implying that security compromises are no longer the exception, but a frequent reality.

Stakeholders are placing increasing pressure on CISOs and their security teams to deliver agility, reduce cost, and keep up with AI's exponential demand. In response, teams are forced into making difficult decisions: prioritising speed over visibility, sidelining data quality, and integrating new environments, very often faster than they can be secured. Much of this is done under the broad and shifting mantra of "acceptable risk", a term that for some organisations changes in meaning and significance depending on the organisation's goals at any given point in time.

As hybrid cloud environments grow more complex and attackers emboldened with AI become more sophisticated, organisations must reflect on an increasingly uncomfortable truth: the more they continue to compromise today, the harder it becomes to meet the challenges of tomorrow.

Compromises are in fashion

Though this would have been unimaginable years ago, security leaders are being pressured into making compromises, often in a deliberate and calculated manner. As cloud environments expand, AI deployments accelerate, and infrastructure grows more fragmented by the day, the demand on security teams now exceeds what existing tools and architectures were ever built or conceived to manage.

Our latest Hybrid Cloud Security Survey, which featured responses from over 1000 security and IT leaders, shows that these trade-offs are often happening in the most critical areas. Nearly half of the respondents lack clean, high-quality data to support secure AI workload deployment. The same number of respondents admit to having insufficient visibility across their hybrid cloud environments, particularly in lateral and encrypted traffic, which remains one of the most critical yet worryingly overlooked areas for threat detection.

A further 47% point to tool integration as a key area of compromise, emphasising the strain of managing sprawling and siloed tech stacks that still fail to give comprehensive insight.

The perception of risk is also changing. 70% of Security and IT leaders now consider public cloud infrastructure the most vulnerable part of their environment. Concerns over governance, persistent blind spots, and the difficulty of maintaining control across distributed architectures have replaced the early optimism that once accompanied cloud adoption

The perception of risk is also changing. 70% of Security and IT leaders now consider public cloud infrastructure the most vulnerable part of their environment. Concerns over governance, persistent blind spots, and the difficulty of maintaining control across distributed architectures have replaced the early optimism that once accompanied cloud adoption.

In today's working environment, there is a risk that compromise could become operationalised, and what was once a one-off occurrence could become a constant. The consequences of this will extend far beyond mere tactical inconvenience. Each trade-off will inevitably introduce ambiguity into risk calculations, increasing the likelihood that a blind spot mutates into a breach. Over time, the cumulative effect of these decisions will become clear, with the slow, often imperceptible erosion of security standards that were once considered non-negotiable.

The weeds are coming up through the cracks

The consequences of compromises are gradually starting to becoming increasingly evident across every layer of the organisation. This year, the percentage of organisations reporting a security breach rose to 55%, a 17% increase from last year. Furthermore, nearly half of security leaders told Gigamon that their current tools are falling short in detecting breaches they've faced. These failures are not a result of under investment. Rather, they stem from environments that have outgrown traditional controls, environments where more data, alerts, and tools do not automatically translate into stronger protection.

Despite its popularity among security leaders, acquiring more security tools doesn't always guarantee better defence against cyberattacks. On average, organisations manage 15 different security tools across their hybrid environments. Yet 55% admit those tools are not as effective as they should be. Instead of helping security teams, this tool sprawl often adds friction, expensive tool overlaps and creates gaps. Oversaturation leads to noise rather than insight, and overlapping capabilities generate confusion rather than clarity whilst at the same time increasing costs.

While organisations are managing this complexity, attackers are adapting and accelerating their tactics. This leaves defenders in a constant state of catch-up.

Now, many organisations are having to face the music. The decisions made to sacrifice visibility, data quality, and tool integration are starting to show their impact. No longer able to defer or avoid the reality, organisations must address these issues head-on.

Visibility, the equation balancer

Risk remains obscured without clear insight into where data travels and how it behaves, leaving organisations unable to make any informed, strategic and secure decisions. 88% of Security and IT leaders say access to network-level data is essential for securing AI deployments, which reflects a broader shift in mindset. Traditional telemetry is no longer enough. Organisations now require deep observability – actionable insights to reduce risk and improve governance by integrating network derived telemetry including packets, flows and meta data with existing metrics, events, logs and traces.

Such comprehensive visibility is the only way organisations can know which parts of their environment is secure and which are most vulnerable. It enables organisations to gain the situational awareness that they need to detect and prevent breaches, as well as respond effectively when incidents occur. More importantly, achieving this level of visbility and clarity can help move the industry away from normalising security compromises towards restoring the standards that should never have been negotiable.

The pressure to compromise will not disappear, but neither should the resolve to uphold strong security standards. Refusing to settle for short-term fixes is the first step towards building a strong security posture and long-term resilience.

There is a sequence to creating a cybersecure culture, and no, it does not start with training employees

Although employee awareness is an important part of creating a SECURE culture, it is not the cornerstone everyone believes.

BY RENE-SYLVAIN BEDARD, AUTHOR OF SECURE BY DESIGN

IT IS all over the surveys; they all point to the user being the weakest link in the security chain. I disagree. It is a symptom, but not the source.

While some social engineering attacks are precisely built to use our weakest psychological traits, it still does not fall on the user.

Who owns the vision, who decides where the ship goes, and who sets goals and priorities for the entire company? CEOs and owners. This is where culture and guidelines must come from. These are top-down operations, rarely the other way around. Having understood this, why believe that by training the bottom of the pyramid we will solve any cultural problem and make cybersecurity a priority?

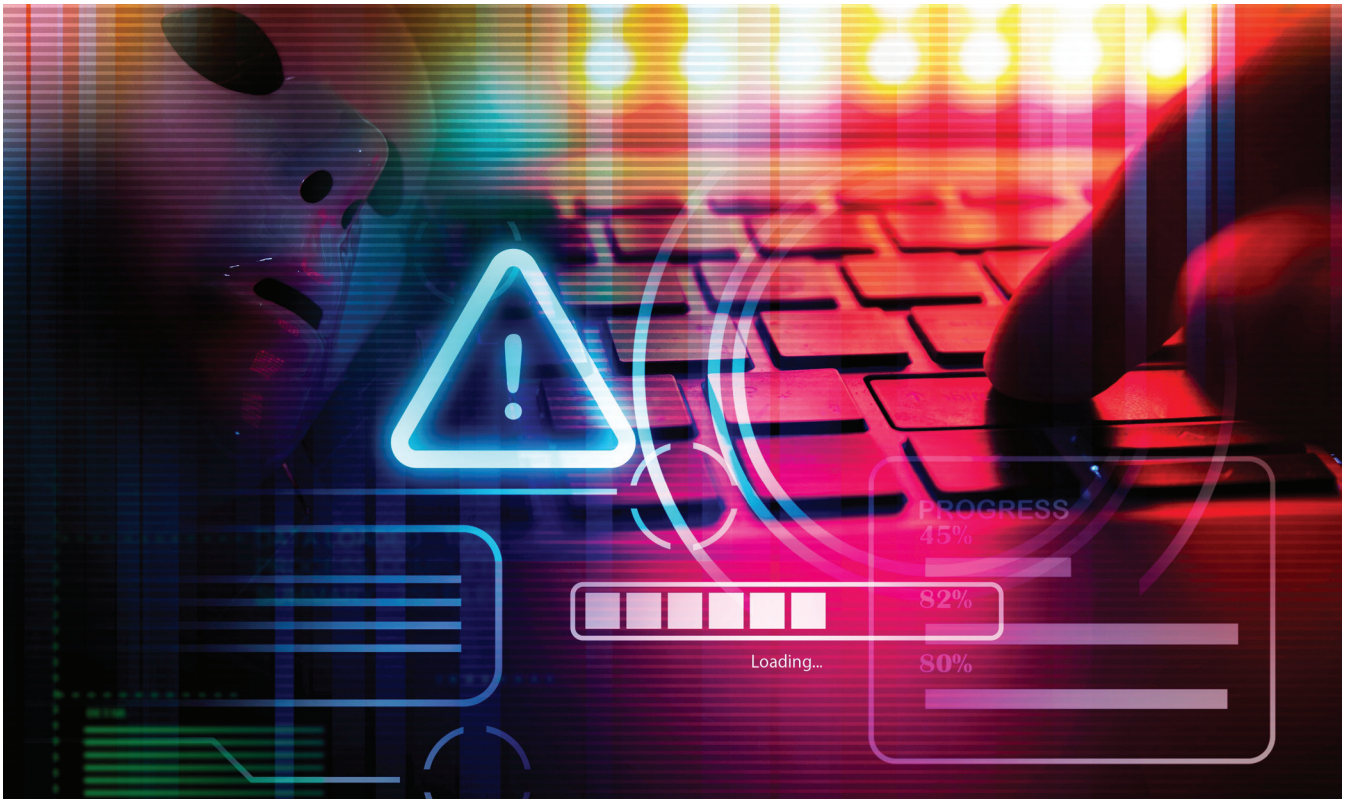
When you answer this one, I believe you will start agreeing with me.

Read the data, but understand the construct

The survey data only explores the result of a cybersecurity incident. Basically, who clicked on the malware, or inserted the USB key found in the parking lot? And yes, at that level, the end user is the culprit. To make sense of the data, you must look at the overall construct.

How did we get to this situation?

My 2 cents, a lack of managerial



courage.

Before you start sending me some hate mail, please hear me out.

Training the end users has its utility, but by itself, it is mainly a waste of time. It needs to be part of a larger, organisation-wide priority.

When leadership decide their yearly priorities, if cybersecurity is not part of that document, it will not exist. Business leaders are the role models of employees; they are the ones to emulate, so if management does not care about cybersecurity, why should the staff?

When KPI return the wrong information

If you have any cybersecurity-related KPIs, you are most likely ahead of the curve, as most companies do not measure their cybersecurity at the executive level, hence it is not part of their reality.

Here's an example: I am standing in front of the management board of a regional authority in healthcare, and I am referring to the numerous cyberattacks that have been fought by their IT team during our audit. They had an average of 10 attacks per week. One of the administrators simply stated: "but we are never under attack, so what are you referring to?" In short, they had no idea. Information does not magically float back to the top. You need to dig for it.

This type of board isolation happens too frequently. The IT teams are fighting to keep the lights on and ensure that cyberattacks don't succeed, but management is kept blind.

In this example, the KPIs were all about uptime and quality of service, not showing any data about cybersecurity and incidents. So here is my question to you leaders, are you even aware of what is happening security-wise, if we take out the number of people that have passed the training?

Here are a few questions that your executives' KPIs should be answering:

- % of identified cybersecurity risks remediated
- Has the monthly cybersecurity drill been successful?
- % of employees signed the new cybersecurity policy and responsible use of technology agreement
- % of executives who have completed their cybersecurity leadership training
- Has the cyber-incident recovery plan been reviewed and updated?
- Are the emergency funds in case of a cyber-incident sufficient?
- How many incidents were detected/remediated last month?

You get the point. There are multiple aspects that must be validated, and that you, as management, should have insight into. Why? Because it directly affects your growth and your bottom line. If you are not secure, then these two things are in danger.

Leaders must become beacons and lead the way. They must be inquisitive about cybersecurity and demonstrate its importance everywhere, might it be in objectives, planning and even reviews. It must become part of the culture, and to do so, it must come from the top. You can't have mixed signals

When leaders need to lead

I might have overstated myself earlier. The fact is, before you start training your staff, your leadership must make cybersecurity a priority. Owners and management teams must be aligned on the importance of security and what needs to be protected at all costs. Leaders must become beacons and lead the way. They must be inquisitive about cybersecurity and demonstrate its importance everywhere, might it be in objectives, planning and even reviews. It must become part of the culture, and to do so, it must come from the top. You can't have mixed signals.

To empower your staff, you need leverage, consistency

So, start demonstrating interest, start surveying your business processes, technologies and people to know, where does criticality lie. Where must cybersecurity be applied, and where do you have blind spots today? Once you know and you have surveyed your environment, you will start seeing a map of areas of your business that you can't live without.

Once you, as the owner, and your management are aligned and have dug enough into your practices, your employees will start noticing that cybersecurity is now important to you.

At that point, it should be part of your dialogues, part of what is important for your company, why it is critical to maintain a healthy digital hygiene, and why some habits may put the company at risk. At that point, you start creating a training portfolio that is fully aligned with your corporate objectives. Then it makes sense.

And what's in it for you, leaders?

Have you ever considered that cybersecurity might be the lever you are missing to unlock those larger accounts that you have been trying to access for years?

This is my hidden gem for you. Those bids that you can't access because you do not have the proper security compliance could open up. A new market of opportunities, where customers are cyber-aware and will want their new partners to demonstrate their cybersecurity.

I can hear you, sure you would like this 7-figure contract, but where to start... Start by contacting me. We will help you go through the SECURE method and will enable this for you.

In the age of GenAI, pre-emptive capabilities, not detection and response, are the future of cybersecurity

By 2030, preemptive cybersecurity solutions will account for 50% of IT security spending, up from less than 5% in 2024, replacing standalone detection and response (DR) solutions as the preferred approach to defend against cyberthreats, according to Gartner.

PREEMPTIVE cybersecurity technologies use advanced AI and machine learning (ML) to anticipate and neutralize threats before they materialize. It includes capabilities such as predictive threat intelligence, advanced deception and automated moving target defense.

"Preemptive cybersecurity will soon be the new gold standard for every entity operating on, in, or through the various interconnected layers of the global attack surface grid (GASG)," said Carl Manion, Managing Vice President at Gartner. "DR-based cybersecurity will no longer be enough to keep assets safe from AI-enabled attackers. Organizations will need to deploy additional countermeasures that act preemptively and independently of humans to neutralize potential attackers before they strike.

"Ignoring the shift brought by AI-driven cyberthreats poses a significant and escalating risk to product and innovation leaders (see Figure 1). By clinging to reactive security strategies as their primary line of defense, they will expose their products, services and customers to a new, rapidly escalating level of danger."

Due to the rapid growth of the GASG, Gartner predicts that by 2030 there will be over 1 million documented cybersecurity Common Vulnerabilities and Exposures (CVEs), up 300% from approximately 277,000 in 2025.

The future of a secure digital world hinges on the commitment to embrace the transformative potential of the Autonomous Cyber Immune System (ACIS) – the ultimate evolution of preemptive cybersecurity for the complex, rapidly growing, GASG.

"The relentless expansion and increasing sophistication of the GASG render traditional, reactive cybersecurity measures obsolete. Though early in its development, the

Figure 1: High-Tech FutureSight: Preemptive Security. Source: Gartner (September 2025)

proactive and adaptive power of the ACIS, is unequivocally the future of digital defense," said Manion. "The development and deployment of intelligent, decentralized, tactical ACIS frameworks are not merely aspirational goals, but an eventual absolute imperative for safeguarding our increasingly interconnected world."

The shift from one-size fits all

There will be a shift from broad, one-size-fits-all DR security platforms toward more targeted and effective preemptive cybersecurity solutions, many of which will be based on agentic AI and domain-specific language models (DSLMs).

This focus on niche areas will present many opportunities for new and existing security vendors to carve out distinct market segments by deeply understanding the unique security challenges of:

- Specific verticals, such as healthcare, finance and manufacturing
- Particular application types, such as industrial control systems, cloud-native applications and AI/ ML pipelines
- Specific threat actor methodologies, such as ransomware targeting critical infrastructure and supply chain attacks on SaaS platforms.

"This emphasis on specialization will drive increased collaboration and integration within the cybersecurity ecosystem. Because no single vendor can effectively address the entirety of the GASG, partnerships and interoperability between specialized solutions will become even more crucial," Manion said.

"For instance, a vendor specializing in preemptive cybersecurity for IoT devices in the healthcare sector might need to integrate with a platform focused on securing cloud-based electronic health records," Manion added. "Such interdependencies will create opportunities for technology alliances, joint go-to-market strategies, and the development of standardized APIs and data formats to facilitate seamless interaction between disparate security solutions."

Worldwide AI spending will total $1.5 trillion in 2025

Worldwide spending on AI is forecast to total nearly $1.5 trillion in 2025 according to Gartner.

Market	2024	2025	2026
AI Services	259,477	282,556	324,669
AI Application Software	83,679	172,029	269,703
AI Infrastructure Software	56,904	126,177	229,825
GenAI Models	5,719	14,200	25,766
AI-optimized Servers (GPU and Non-GPU AI Accelerators)	140,107	267,534	329,528
AI-optimized IaaS	7,447	18,325	37,507
AI Processing Semiconductors	138,813	209,192	267,934
AI PCs by ARM and x86	51,023	90,432	144,413
GenAI Smartphones	244,735	298,189	393,297
Total AI Spending	987,904	1,478,634	2,022,642

Source: Gartner (September 2025)

Table 1: AI Spending in IT Markets, Worldwide, 2024-2026 (Millions of U.S. Dollars).

"The forecast assumes continued investment in AI infrastructure expansion, as major hyperscalers continue to increase investments in data centers with AI-optimized hardware and GPUs to scale their services," said John-David Lovelock, Distinguished VP Analyst at Gartner. "The AI investment landscape is also expanding beyond traditional U.S. tech giants, including Chinese companies and new AI cloud providers. Furthermore, venture capital investment in AI providers is providing additional tailwinds for AI spending."

Looking towards 2026, overall global AI spending is forecast to top $2 trillion, led in large part by AI being integrated into products such as smartphones and PCs, as well as infrastructure (see Table 1).

Top emerging technologies to support autonomous business

Gartner has unveiled the 2025 Hype Cycle for Emerging Technologies. Many of the top technology innovations to watch this year support the new autonomous business era, including machine customers, AI agents, decision intelligence and programmable money.

Gartner Hype Cycles provide a graphic representation of the maturity and adoption of technologies and applications, and how they are potentially relevant to solving real business problems and exploiting new opportunities. Gartner Hype Cycle methodology gives a view of how a technology or application will evolve over time, providing a sound source of insight to manage its deployment within the context of specific business goals.

Speaking at the recent Gartner IT Symposium/Xpo on the Gold Coast, Australia, Marty Resnick, VP Analyst at Gartner, said, "After years of digital transformation, organizations now face new disruption as AI and automation reshape competition, customers, products, operations and leadership. In this new autonomous business era, CIOs must assess how emerging technologies can create competitive differentiation, unlock greater efficiencies and capture new growth opportunities."

The Hype Cycle for Emerging Technologies is unique among Gartner Hype Cycles because it distills key insights from more than 2,000 technologies and applied frameworks that Gartner profiles each year into a succinct set of "must-know" emerging technologies. These technologies have potential to deliver transformational benefits within the next two to 10 years (see Figure 1).

Machine Customers

Machine customers are nonhuman economic actors that purchase goods or services on behalf of people or organizations. Gartner estimates three billion B2B internet-connected machines can act as customers today, growing to eight billion by 2030. Examples include virtual personal assistants, smart appliances, connected

cars and Internet of Things (IoT)-enabled factory equipment.
"Machine customers will play an important role in industries like manufacturing, retail and consumer goods, unlocking new revenue and efficiency opportunities," said Resnick. "To capitalize, organizations must reimagine their business models or risk being left behind."

AI agents

AI agents can perceive, make decisions, take actions and achieve goals in their digital or physical environments to help organizations meet their objectives. By using tools like LLMs, organizations are creating and deploying AI agents to handle complex tasks. These agents could transform many industries by automating work in areas like consumer services, industry, data analysis, content creation and logistics.

Trust in AI agents remains limited due to concerns about their ability to accurately predict and execute tasks. Without human oversight, AI agents could make important decisions quickly before anyone notices. Gartner recommends organizations factor AI agents into strategic planning by understanding their capabilities and applications, especially as they become more independent and easier to use.

Decision intelligence

Decision intelligence is a practical discipline that advances decision making by understanding and engineering how decisions are made, as well as how outcomes are evaluated, managed and improved via feedback. By digitizing and modeling decisions as assets, it bridges the insight-to-action gap to continuously improve decision quality, actions and outcomes.

"Agentic AI and generative AI hype, regulatory pressures on decision automation and recent global uncertainty have revealed weaknesses in traditional business processes and decision making," said Christian Stephan, Senior Director Analyst at Gartner.

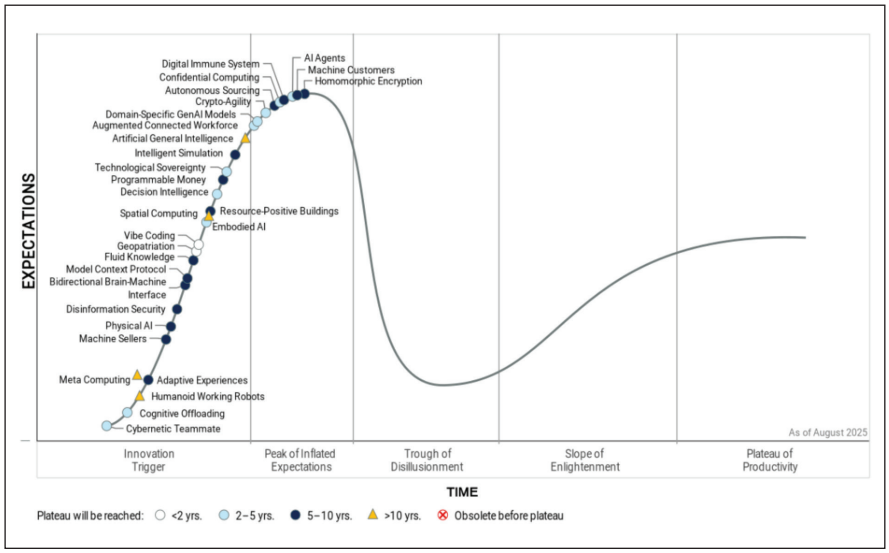
"In response, organizations now demand decision processes that deliver speed and quality, but are also consistent, compliant, cost-effective and capable of handling complexity and change."

Programmable money

Programmable money is any form of digital money that can be programmed using software that determines its operation based on algorithmic criteria. It can rely on blockchain-enabled tokenization and smart contracts to increase the participation of economic actors and program value exchanges.

Organizations will be required to engage with programmable money to connect with machine customers as new types of customers, as well as business peers and employees.

"Programmable money is transformative for financial services providers, enabling new forms of currency and digital asset markets," said Stephan. "It drives innovation in value creation, financing, and asset exchange, including machine-to-machine trading, reshaping supply and financial value chains."



➤ Figure 1: Hype Cycle for Emerging Technologies 2025.
Source: Gartner (September 2025)

Organizations must develop a "Risk Reflex"

To thrive in today's rapidly evolving risk environment, risk, audit and compliance leaders must develop "reflexive risk ownership" - a future state where business leaders instinctively and automatically recognize, respond to, and manage risks, according to Gartner, Inc., a business and technology insights company.

During the opening keynote at the recent Gartner Enterprise Risk, Audit & Compliance Conference today, Gartner experts said organizations now face risks that emerge quickly, are highly interdependent, and are increasingly difficult to classify, making this shift in risk management more critical than ever.

"Risk management is now one of CEOs' most critical priorities; its importance has increased by over 50% since last year," said Chris Audet, Chief of Research in the Gartner Assurance Practice. "This has created a unique moment for assurance leaders."

To develop an organization's risk reflex will require a mix of coaching risk owners and leveraging advancements in enterprise technology, particularly AI. "Eighty-eight percent of risk owners are highly motivated to meet expectations around managing risks," said Tegan Gebert, Vice President in the Gartner Assurance Practice. "Yet only 35% feel confident they know how to do so. They need assurance leaders to show them how."

Chris Audet, Chief of Research and Tegan Gebert, Vice President in the Gartner Assurance practice presenting the opening keynote today at the Gartner Enterprise Risk, Audit & Compliance Conference in Grapevine, Texas.

Coaching

Much like a sports coach is responsible for creating the systems, stimuli, and structures that foster great athletes, assurance leaders must coach their risk owners to develop a risk reflex.

To coach an organization towards having a risk reflex will involve deliberate, marginal steps towards a

> “Assurance leaders need to be the coaches their risk owners need: leveraging tools, insights and influence to get them to practice, to improve, and to persist, an organizational risk reflex will be enabled by a series of actions that are learned or practiced until they happen so automatically that they appear reflexive. Assurance leaders must create the larger system that both encourages and reinforces the right risk ownership behaviors”

larger goal.

“Assurance leaders need to be the coaches their risk owners need: leveraging tools, insights and influence to get them to practice, to improve, and to persist,” said Gebert. “An organizational risk reflex will be enabled by a series of actions that are learned or practiced until they happen so automatically that they appear reflexive.

“Assurance leaders must create the larger system that both encourages and reinforces the right risk ownership behaviors.”

To transform risk management into something as natural as a learned reflex, Gartner experts recommend assurance leaders focus their efforts on three building blocks.

Three foundations of an organizational risk reflex

1. Engineer: The first foundation is on engineering systems that make the right risk behaviors both easy to perform and difficult to ignore.

“Small, deliberate changes in environment and process can drive large improvements in outcomes. Assurance leaders are already simplifying guidance, streamlining documentation, and integrating risk considerations into everyday workflows,” said Audet.

“However, making things easier is not enough—systems must also be engineered so that compliance is prominent, expected, and socially reinforced. This means making risk actions hard to miss, hard to justify avoiding, and hard to hide.”

For example, Gartner experts foresee an environment where vendors offer contract management systems that double as a third-party risk management platform. This would enable a risk owner to renew a contract or choose from a pre-approved list of suppliers, without long due diligence checks. Compliance would be hard to avoid, and it would improve risk management.

2. Provoke: The second foundation is to intentional provocation; creating stimuli that prompt risk owners to think deeply and act decisively.

“Assurance leaders must design interactions – risk assessments, workshops, and feedback sessions, for example – that challenge conventional thinking, encourage candid discussions, and share novel, actionable insights,” said Gebert.

Examples include asking more thought-provoking questions in risk surveys, or planning audits to be focused on what is novel or insightful – auditing the underlying project environment, for example, rather than just project governance.

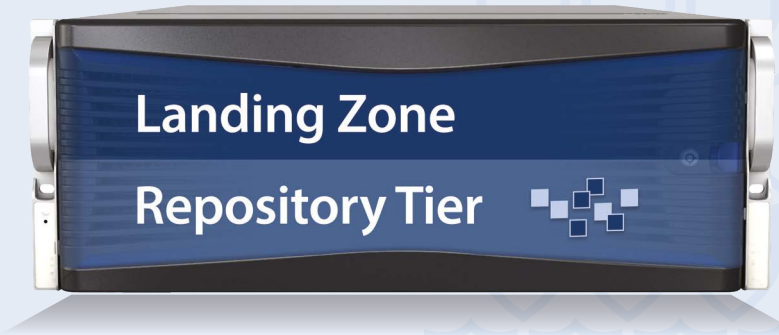
3. Recognize: The third foundation reinforces the right risk behaviors by putting in processes to make them visible and rewarding.

“Positive reinforcement – through visible, public acknowledgment – helps create and strengthen the neural pathways that turn good risk behaviors into habits. Recognition should focus on effort, transparency, and continuous improvement, not just perfect outcomes,” said Audet. “Assurance leaders are uniquely positioned to define and elevate such behaviors.”

Examples include celebrating proactive risk management, sharing successes across teams, and using dashboards and recognition platforms to highlight exemplary behaviors.

EXAGRID®

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

WINNER
SDC AWARDS 2023

- **Storage Company** of the Year
- **Backup/Archive Innovation** of the Year

Thank you so much to all who voted, and congratulations to our fellow SDC Awards 2023 winners!

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

LEARN MORE >