Security Industry

TRENDS REPORT

2026

GALLAGHER Security

January 2026 Author: Rachel Akbar Design: Jason Lurman

Contents

Clarity for the Year Ahead

Each year, this report offers more than insights, it offers perspective. It helps us step back from the noise and chart the direction our industry is truly taking, and in 2026, that direction is becoming clearer than ever. Security is no longer operating at the edge of an organization; it's moving to the center of how businesses work, plan, and make decisions.

Security has always been essential, and now it's increasingly becoming strategic. Across this year's findings, leaders are asking new questions: How can security reduce complexity? Where can it create time and clarity? How does it help us work more efficiently and confidently? How does it improve profitability? These aren't questions about technology for technology's sake - they're questions about impact. And they reflect a shift in how organizations perceive the value of what we do.

Over the last two Trends Reports, we've seen businesses strengthen their foundations and begin reimagining what their systems could deliver.

This year, we see something more: a growing belief that security can be a driver of performance. Integration is being recognized for its return on investment. Data is becoming a shared language between security, IT, and operations. And partnership - between manufacturers, integrators, consultants, and customers - continues to be the anchor that helps teams navigate complexity with confidence.

Of course, the challenges remain real. Workforces are stretched, cyber risks are evolving, and new technologies arrive faster than many organizations can absorb. What encourages me is the adaptability and curiosity I see across our industry. The willingness to learn, to collaborate, and to rethink long-held assumptions is what will carry us forward.

My hope is that this report brings clarity that helps you make decisions far beyond traditional security, and into the higher value outcomes you want to unlock more of.

Because when we understand the full potential of security as a strategic enabler, we open the door to possibilities far greater than the technology itself.

Mark Junge
Chief Executive

Executive Summary

A year of recalibration lies ahead.

With global volatility and changing political environments, organizations are reevaluating how and where they invest. At the same time, decision-making is becoming increasingly complex as more stakeholders become involved. End Users need support understanding the value and impact of security, creating new opportunities for Channel Partners and Consultants to step in with guidance.

Upgrades under pressure

Hardware and software upgrades remain top priorities for End Users, reflecting an industry still intent on reinforcing its foundational systems. Yet as financial scrutiny intensifies, so does the pressure to demonstrate clear, measurable returns. Those who can articulate business value beyond basic protection are best positioned to secure investment and support.

Decision-making grows more complex

Security purchasing decisions are no longer made in isolation. With more stakeholders involved, the definition of value is shifting, and ease of use, support, and communication now carry as much weight as the technology itself. As a result, navigating the buying process has become increasingly complex.

Integration defines business value

Integration is now the leading factor in End Users' security system decisions. By connecting with existing systems and generating actionable data, integrated solutions are delivering measurable business value, shifting security from an operational cost to a strategic investment.

Support becomes a strategic differentiator

Persistent staffing and skills shortages continue to plague the industry, influencing everything from system design to post-deployment support. As a result, many are turning to manufacturers for help - through training and ongoing support - cementing the view that partnership is moving beyond a value-add to a strategic differentiator.

ROI emerges as security's north star

As the industry recalibrates for 2026, the lens through which success is measured is changing. Return on investment is no longer just a finance metric - it's becoming the common language connecting security teams with broader organizational goals. Demonstrating ROI now means showing how security contributes to organizational resilience, operational efficiency, and strategic growth. Those who can quantify this value will not only secure budgets, but elevate security's role at the executive table.

2025 vs. 2026

The 2026 survey results reveal an industry balancing familiarity with fresh challenges. While priorities like video integration and mobile credentials continue to dominate discussions, tightening budgets and economic pressures are beginning to reshape organizational strategies and expectations.

What's continuing

Moderate mobile credential adoption

End Users continue to show slow adoption of mobile credentials with 48% of respondents saying they're unlikely to employ them in 2026 compared to 2025's 27%. However, there was an increase in those who said they are likely to adopt (39% this year compared to 33% in 2025). With 13% reporting that they've already adopted mobile credentials, if the industry can figure out how to remove some of the barriers to uptake, we may see that number increase over the next few years.

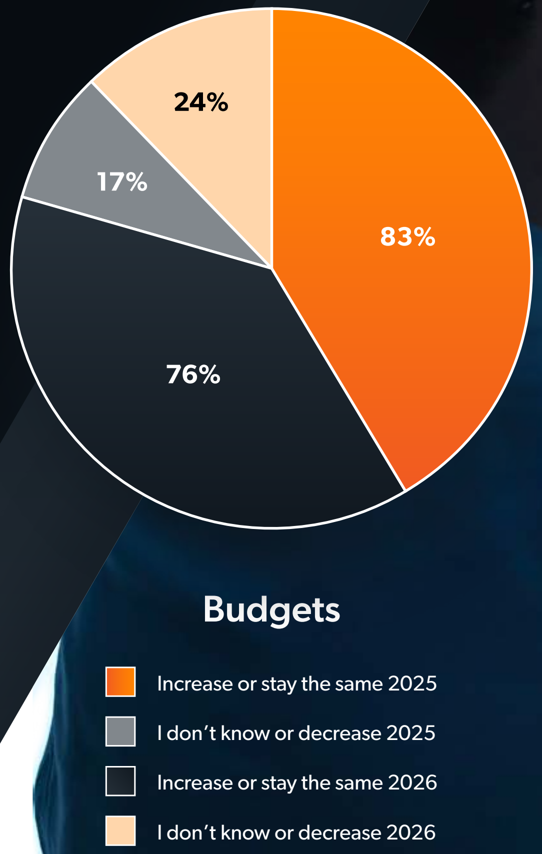
Video integrations are prioritized

Across the board, video continues to be the top integration priority for both End Users (25%) and Channel Partners (26%).

What's changing

Budgets are constrained

Budgets remained stable in 2024 and 2025, but in 2026 we're seeing them begin to decline. Most survey participants (24%) named overcoming budget constraints as their top organizational challenge; pair this with the economic uncertainty caused by tariffs and geopolitical tensions and the data paints a picture of a security industry under pressure to deliver a return on investment *(International Monetary Fund,* 2025*)*.



Shaping the Digital Frontier: Data Centers and AI

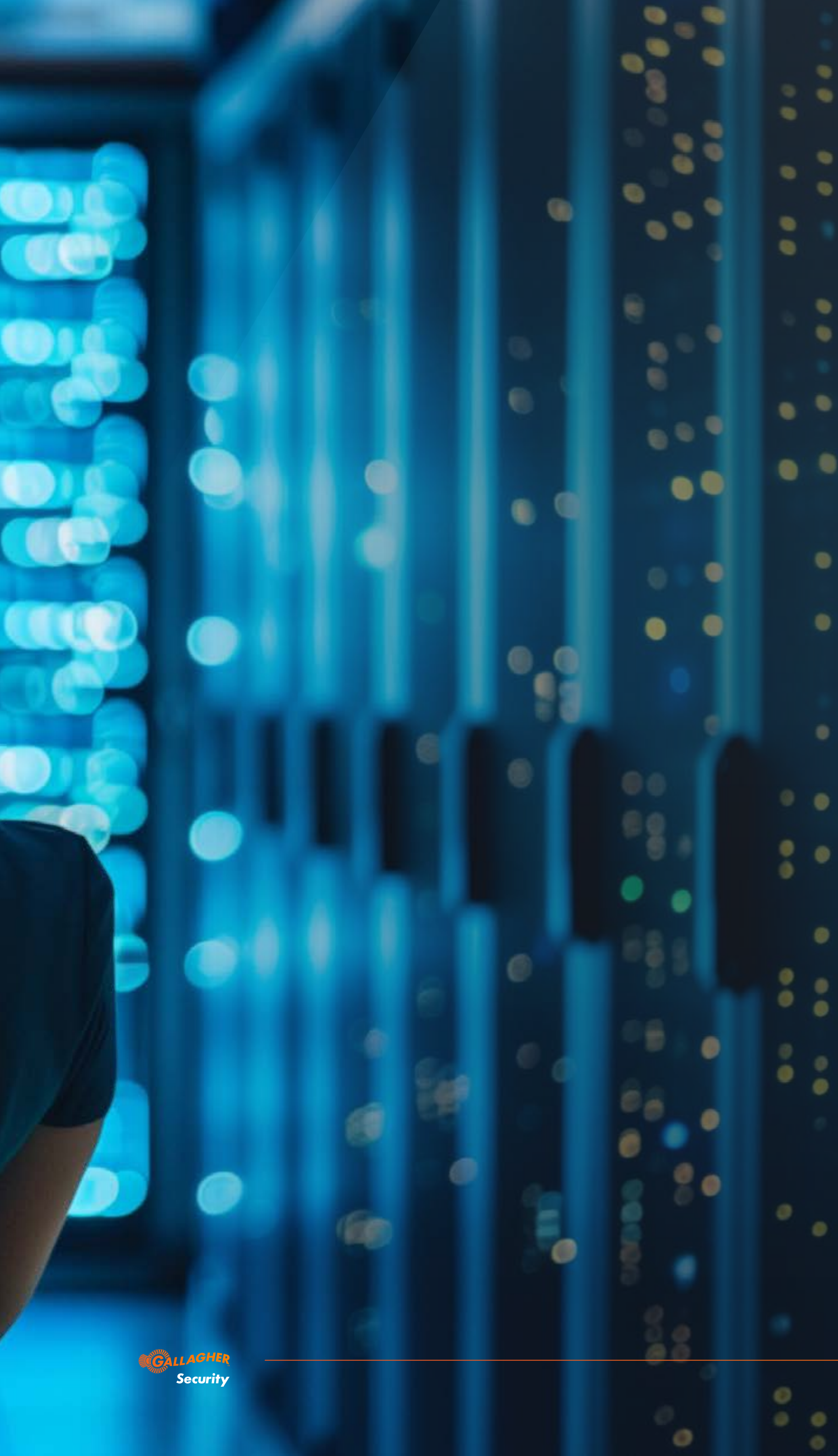
AI stole the spotlight in 2024, and in 2025, data centers took center stage as the backbone of digital transformation and one of the most consequential markets shaping the global economy.

There are now nearly 12,000 data center facilities worldwide, with almost half located in the United States - and that number is growing fast (Alaameer, 2025). Global investment in data infrastructure is projected to grow at a compound annual rate of 11.7%, reaching $584.86 billion USD by 2032 (*Data Center Market Size, Share & Industry Analysis*, 2025).

The impact of that growth is already visible. Nearly all U.S. economic growth in the first half of 2025 stemmed from investment in data centers and information technology infrastructure; remove those, and growth would have stalled at just 0.1% (Lichtenberg, 2025).

It's no wonder that Channel Partners and Consultants named data centers among their top three fastest-growing vertical markets in our survey, with participants in the Americas ranking it second only to education.

The implications for the security industry are profound. As AI drives a new wave of digital infrastructure, the physical and cybersecurity of these facilities are moving into sharper focus.



What's driving growth?

To put it simply, the digital transformation.

The move toward cloud services, the rollout of 5G networks, and of course, the increased use of AI have all accelerated the expansion of data centers (*Data Center Market Size, Share & Industry Analysis*, 2025). By 2027, AI technologies are expected to account for 28% of global data center activity, more than double what they are today (*How AI is transforming data centers*, 2025).

That demand isn't merely theoretical: 44% of End Users in our survey reported implementing AI tools in 2025 - a 42% increase from 2024 - and they're using them primarily for video analytics and operational efficiency. However, expectations are that AI and security solutions will deliver automation, proactive alerts, and predictive threat intelligence in the near future.

Challenges

Growth at this scale brings growing pains.

Power and grid constraints

Rising electricity demand and grid bottlenecks are delaying nearly 20% of planned data center projects, with major hubs in Amsterdam, Dublin, and Singapore pausing new builds to manage limited power capacity (D'Ambrosio et al., 2025).

Cooling efficiency and water usage

Cooling remains a top operational and sustainability challenge, as the shift to liquid cooling improves efficiency but raises new cost, maintenance, and compliance pressures under tightening environmental regulations (D'Ambrosio et al., 2025).

Location and infrastructure rigidity

Despite opportunities to expand elsewhere, most new data centers still cluster in established hubs, creating congestion and limiting flexibility as data sovereignty and latency concerns restrict movement to lower-cost and lower-density regions (D'Ambrosio et al., 2025).

Opportunities

Even as pressures mount, the data center boom presents clear opportunities for those positioned to help secure and sustain it.

Securing infrastructure

Data centers face a high degree of cyber-physical risk, creating opportunities for security providers to lead the convergence of monitoring, cybersecurity, and access control platforms.

Sustainability and operational intelligence

Security providers can help data centers turn their systems into ESG tools, using access control and IoT data to track energy, occupancy, and sustainability performance aligned with global standards.

Turning compliance into competitive advantage

As data centers face increasing scrutiny from regulators and tenants alike, security providers can differentiate by helping operators strengthen assurance frameworks, integrating security systems that deliver verifiable audit trails, meet standards like ISO 27001 and SOC 2, and demonstrating measurable proof of protection to a variety of stakeholders.

When energy becomes a security imperative

Every era of innovation has been defined by its energy source. The first industrial revolution was fueled by coal, the digital revolution by fossil fuels, and as we further enmesh ourselves in the data revolution, it's clear that renewable energy must become the foundation for the next wave of progress.

As such, we find ourselves at a crossroads. We have the knowledge and the technology to make renewables like solar, wind, and hydro our primary energy sources, but our infrastructure hasn't kept pace. The hurried adoption of AI, cloud computing, and data-intensive operations has outgrown what aging power grids were designed to handle, putting new pressures on both capacity and reliability.

Despite its challenges, energy independence may offer the most practical path forward for industries like data centers. On-site generation through microgrids and emerging technologies like compact, next-generation reactors can help organizations reduce their reliance on overstretched grids while supporting sustainability goals.

Managing and distributing data at scale requires rethinking traditional models that rely heavily on conventional power sources like coal, gas, and nuclear. A simplified approach involves decentralizing capability by deploying micro data center pods, compact units roughly the size of a parking space strategically placed in high-demand zones. These pods can alleviate pressure on main data centers, reduce latency, and enable localized resilience.

Producing power on-site changes the security equation. It introduces new intersections between physical protection, regulatory oversight, and cybersecurity. As energy systems modernize, so must the safeguards around them. The next phase of resilience will be defined by trust and assurance, demonstrating not just that systems work, but that they're verifiably secure, monitored, and accountable.

When power generation moves inside the perimeter, protection must follow. Resilient infrastructure will depend on layered defenses, zero-trust principles, and a unified approach to managing risk across both digital and physical domains.

Modernization is no longer about how much power we can produce - it's about how confidently we can protect it. And the leaders of tomorrow will be those who recognize that shift in perspective.

Jeff Fields

Director of Government Programs - the Americas

Investment Outlook: Channel & End Users

The industry's near-term goals aren't about chasing the newest technology: they're about building foundational and interoperable platforms that will make innovations like AI, mobile credentials, and cloud achievable at scale.

Investment priorities

Across the board, Channel Partners are closely aligned with the investments End Users are prioritizing going into 2026, a sign of strong communication and a shared understanding of customers' needs.

Channel says End Users will prioritize:

1. Hardware upgrades
2. Video surveillance
3. Software upgrades
4. Analytics
5. Cybersecurity fortification

End Users report they'll prioritize:

1. Hardware upgrades
2. Software upgrades
3. Video surveillance
4. Analytics
5. Intruder detection

What they're *not* prioritizing

However, what organizations aren't investing in tells an equally important story, one of an industry still focused on mastering the fundamentals. The emphasis on upgrades signals that many End Users are still stabilizing legacy environments and preparing their infrastructure for more advanced, connected technologies.

In other words, for many, digital transformation remains on the horizon, not yet fully realized.

End Users' least important investment priorities:

1. Cloud capabilities
2. Biometric capabilities
3. Mobile credentials
4. Cybersecurity fortification
5. Perimeter protection

Channel understand End Users' lowest access control priorities, but are less aligned on the rest:

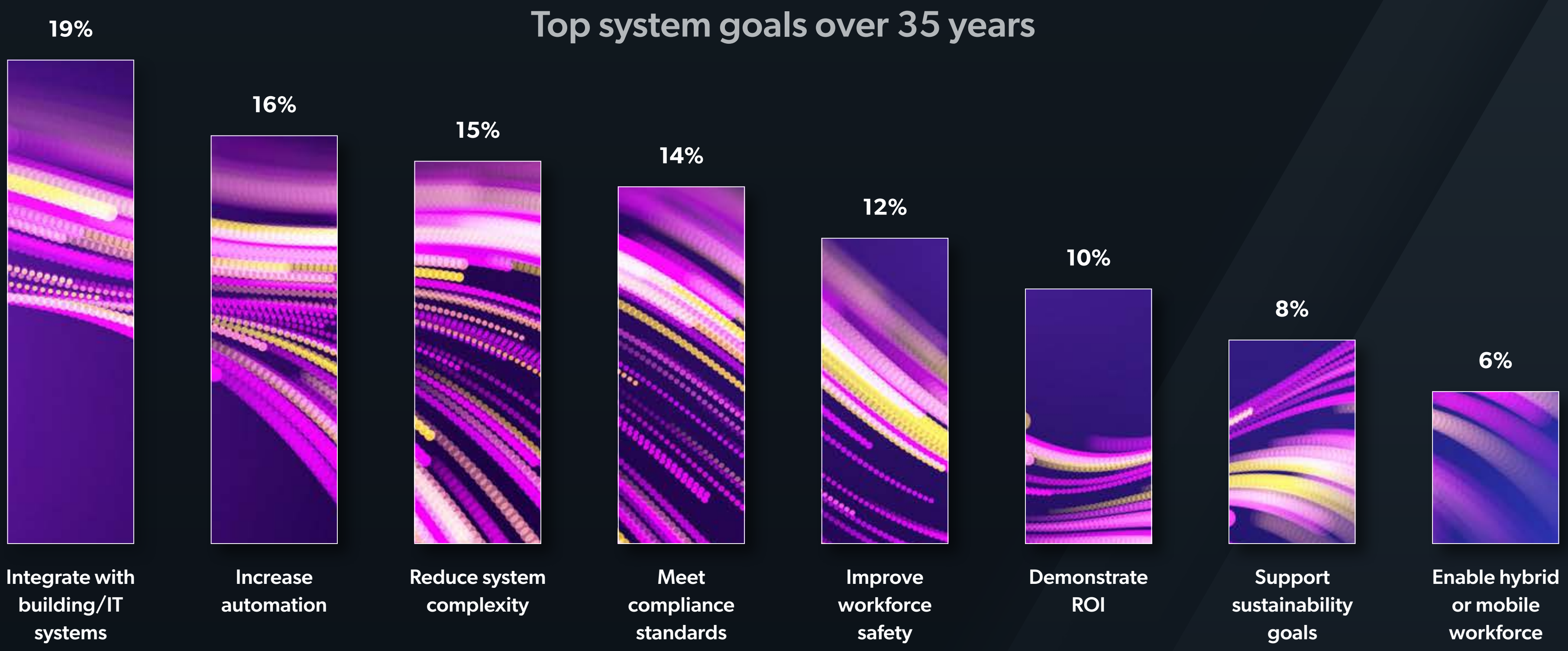
1. Intruder detection
2. Mobile credentials
3. Incident management
4. Perimeter protection
5. Biometrics

Notably, this question allowed participants to select multiple responses from a predefined list but also included a write-in option. Of those who chose to elaborate, both Channel and End Users overwhelmingly named cost savings as a top priority, a factor that may explain the focus on upgrades and efficiencies over newer technologies.

System goals

Looking ahead 3–5 years, organizations are setting their sights on stability, simplification, and measurable performance.

Collectively, these priorities reflect an industry focused on building unified, efficient, and compliant systems that deliver tangible business value. Security leaders are under pressure to do more with less, and that's shaping a year ahead where integration, automation, and cost-efficiency define success.



Top system goals over 35 years

Uncovering new value

When it comes to unlocking greater value from existing systems, there's a noticeable gap between perception and practice.

63% of Channel Partners, Consultants, and Technology Partners say they actively help their customers find new value in their systems. Yet only 37% of End Users report having strategies in place to do the same, with the remainder either not pursuing such efforts or unsure if they exist.

This disconnect underscores an opportunity: as budgets tighten and return on investment becomes a defining metric, the ability to reveal hidden value in existing systems may be security providers' most powerful differentiator in the years ahead.

The quiet power of Channel

There's a misconception that innovation flows from the top down, from manufacturers to end customers with Channel Partners somewhere in the middle. But anyone who's spent time on the ground in this industry knows that's not how it really works.

The most meaningful advancements often begin with Channel's curiosity and the questions they ask on behalf of their customers. Why are people struggling with this feature? How could this process work better? What are we missing? Those conversations reveal gaps that spark new approaches, influencing both technology development and strategy.

Channel Partners are the industry's greatest multipliers. They see across verticals, geographies, and technologies, giving them a panoramic view of the market few others possess. They see how systems behave under pressure, why integrations succeed, and where organizations are quietly creating new efficiencies of their own.

That breadth of experience makes Channel one of the most underutilized sources of insight and foresight in security. Manufacturers who tap into that knowledge gain more than feedback - they gain early awareness of customer needs, guidance that accelerates development, and relationships that turn adoption into advocacy.

Channel isn't just one link in the chain; they're the multiplier that makes the whole chain stronger. They amplify innovation, distribute knowledge, and ensure that progress scales beyond individual projects to reshape entire markets.

For years, we've measured Channel by their ability to close deals. The time has come to measure them by their ability to open possibilities.

Sam Gibbons

Marketing and Engagement Manager – APAC & IMEA

People

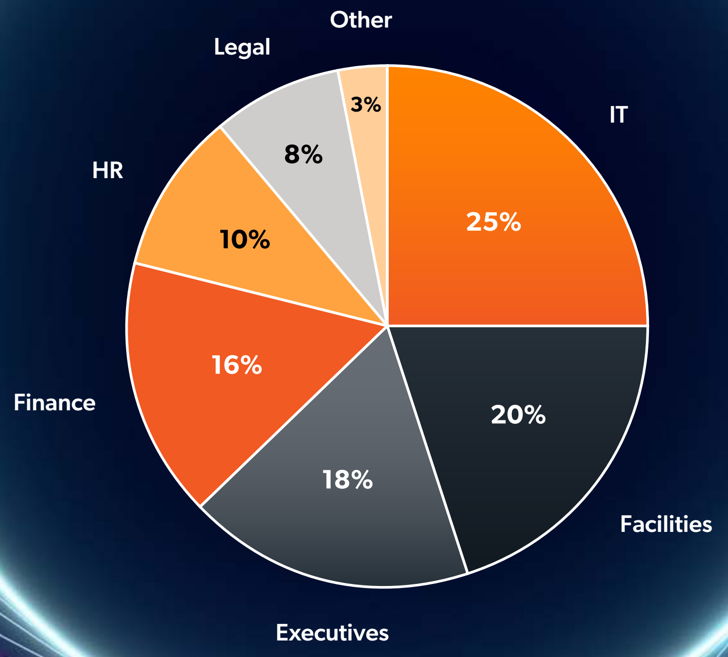
From influencing purchasing decisions to the growing need for support and training, it's clear that success in security depends as much on empowering people as it does on advancing technology.

Purchasing decisions broaden

Decision-making around security systems is no longer confined to security departments. Nearly two-thirds of both Channel Partners (61%) and End Users (64%) say non-security teams now influence purchasing decisions, signaling a clear shift toward multidisciplinary decision-making.

IT has emerged as the most influential stakeholder, reflecting the growing convergence of cyber and physical security, while facilities, executives, and finance also play strong roles, showing that investments are increasingly weighed against strategic value. The inclusion of HR and legal points to rising attention on people, privacy, and policy alignment.

Purchasing Decision Makers



Support and communication

When it comes to selecting a manufacturer or recommending a system, Channel Partners and Consultants rank support as the number one deciding factor, followed closely by communication, underscoring the importance of accessible expertise and responsive partnerships.

Challenges

For Channel, staffing and skills shortages remain the top challenge, with 24% of respondents citing it as their biggest hurdle.

While budget constraints dominate End User concerns, 22% also identified staffing and skills shortages as major issues. Notably, 18% of respondents said balancing technological complexity with convenience is their third biggest challenge, followed by resistance to change (14%). Altogether, it paints a picture of organizations struggling to navigate workforce limitations while managing broader system use, stakeholder involvement, and evolving technology.

Training and upskilling needs rise

To bridge the gap, 61% of both Channel and End Users are turning to training. Of those, nearly a third are specifically relying on manufacturer-led programs.

However, there's growing recognition that training alone can't solve it all. 16% of respondents said they're turning to automation to reduce manual workloads, while 14% are diversifying hiring practices to attract new skillsets. Concerningly, 8% admit they're not currently addressing their staffing and skills gaps at all, signaling a potential risk to both service quality and innovation across the industry.

Despite these options, several participants say they're taking more extreme measures such as *"reducing the manufacturers on our approved vendors list," "approaching staff from other customers/competitors,"* and *"using contractors to keep our security systems working."* Others noted a deeper challenge, saying there's *"not enough interest"* to attract new talent *"or even [enough people] currently in the industry to upskill,"* pointing to a larger systemic issue boiling over.

The talent we've been overlooking

The conversation about staffing shortages has become too familiar. Every year, we talk about the lack of technical skills, the need for more training, and the struggle to attract new talent. But what if part of the problem isn't the shortage itself, but how narrowly we've defined who belongs in security?

For decades, we've looked inward to fill our ranks, hiring those with security backgrounds, certifications, or experience with similar systems. It's a logical approach, but it also limits us. The truth is, the next generation of talent might not come from security at all.

Our industry is built on problem-solving, risk assessment, and critical thinking, all qualities that exist in abundance across countless other professions. The analytical mindset of an engineer, the empathy of a teacher, the composure of a paramedic, or the creative reasoning of a designer are exactly the capabilities that modern security demands. As technology evolves and systems become more interconnected, we need people who can connect ideas just as effectively as they connect hardware.

Attracting this kind of talent requires a shift in mindset. It means redefining security as a creative and dynamic industry, not just one of compliance and control. It means designing entry points for people who may not know they already have the skills we need. It also means rethinking training as an opportunity to attract those newcomers eager to contribute.

None of this diminishes the experience or expertise of those who've built this industry. Their work created the standards, systems, and trust that make modern security possible. But the next step is ensuring that legacy continues by expanding the circle to include new thinkers who can carry it forward. Because when someone outside the industry joins our ecosystem, they bring a fresh way of thinking. They challenge assumptions, spot inefficiencies, and ask the questions we've stopped asking. That's how transformation happens.

When we broaden our definition of who belongs here, we don't just solve a staffing problem. We invite the talent who will take our industry further than we've imagined.

Scott Bell

Training Solutions Lead

Shifting Foundations

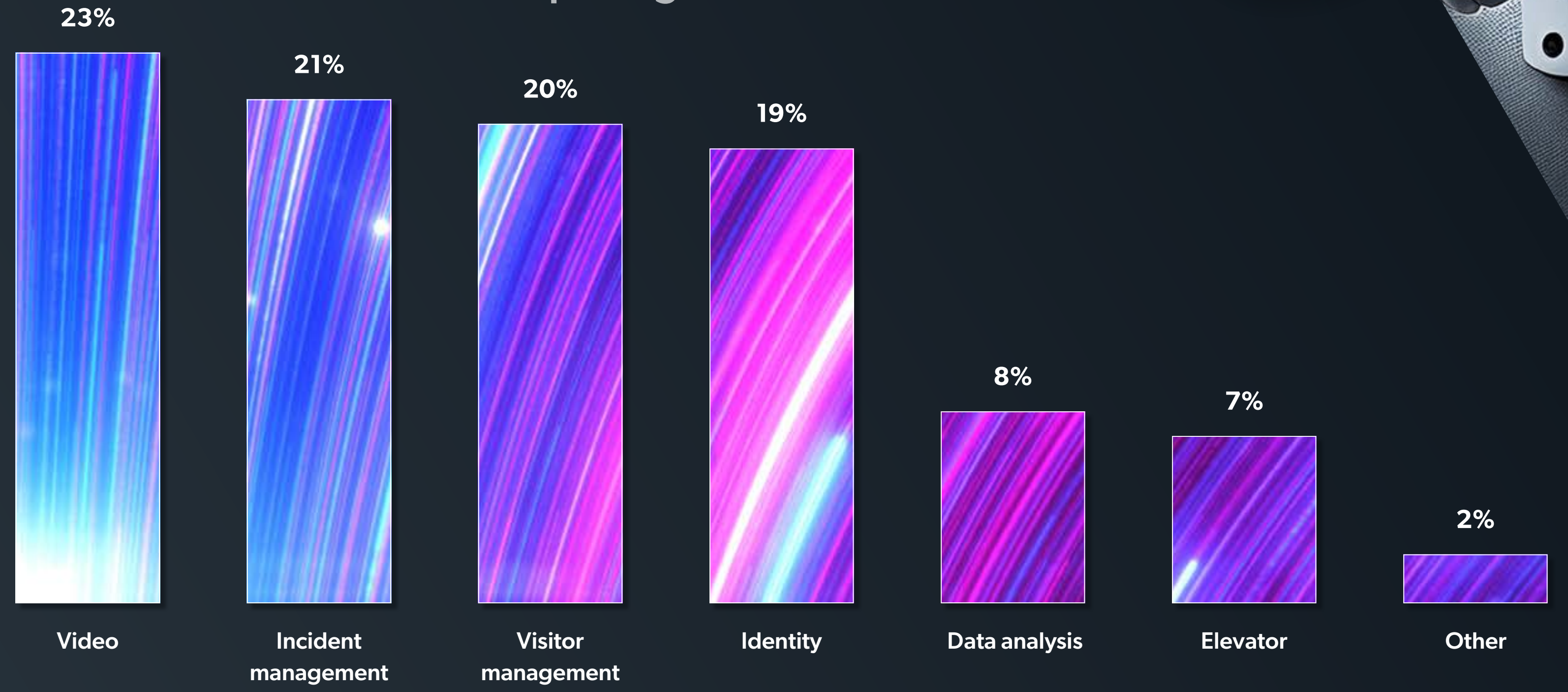
As organizations move deeper into the digital transformation, the foundations of security are shifting. End Users prepared to make the leap are demanding stronger integrations, help developing clearer cloud strategies, and greater confidence in cybersecurity, all while grappling with the pace of technological change.

Integrations driving decision making

For End Users, integration now defines system choice. It ranked as the #1 deciding factor when choosing a security solution, with respondents emphasizing the importance of connected ecosystems over individual features.

This continued focus on video and incident management suggests End Users are looking to unify operational visibility and response under one platform, an evolution from 2025's emphasis on video as a stand-alone priority.

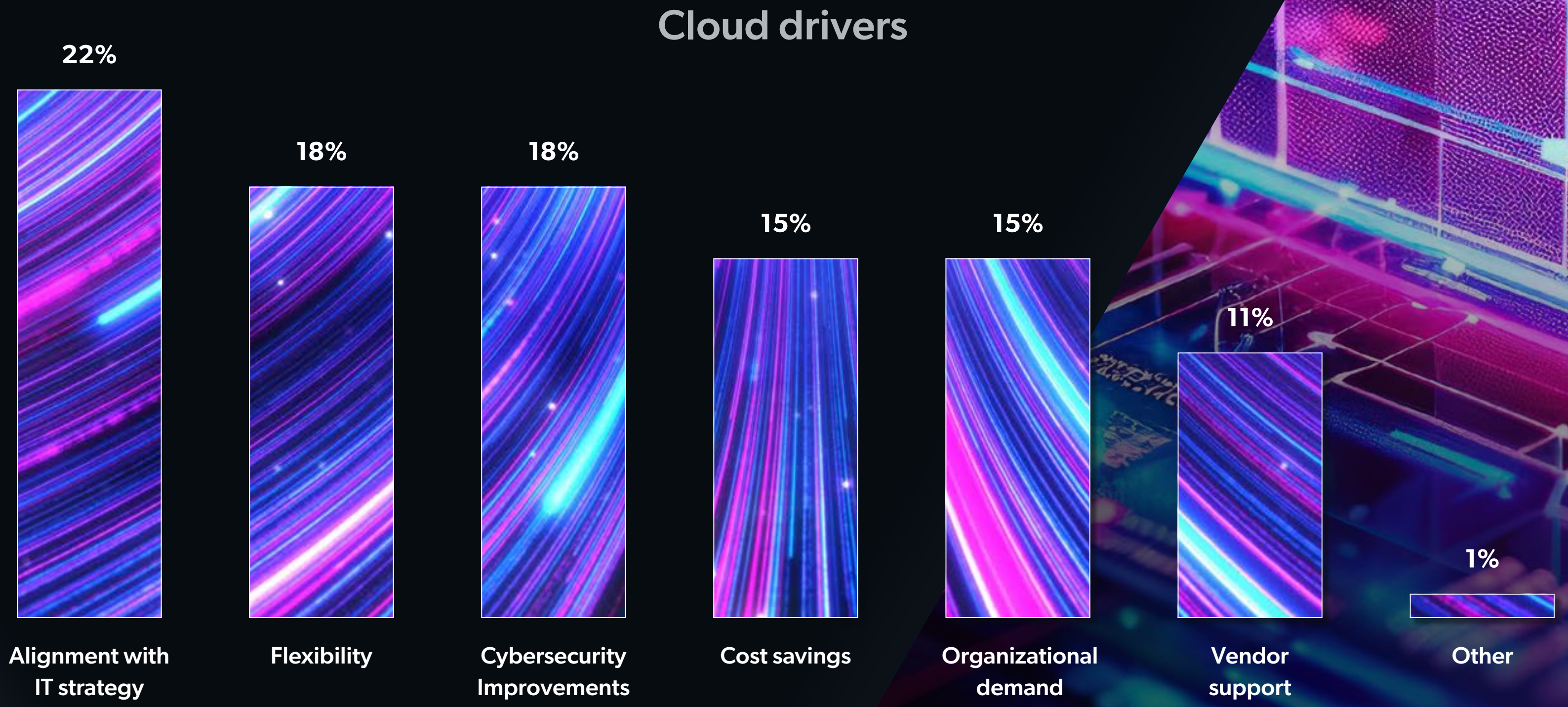
Top integrations for End Users



Trust and education key for cloud

Nearly half of End Users (47%) say their organizations have strategies for cloud deployment, with similar agreement from Channel Partners (45%) who report their customers do, too.

The motivations driving cloud strategy echo the same forces shaping purchasing and investment decisions: the need for alignment with IT, flexibility across systems, and stronger cybersecurity postures. Together, these priorities point to a market where ease of use and long-term integration value are beginning to outweigh short-term cost considerations.



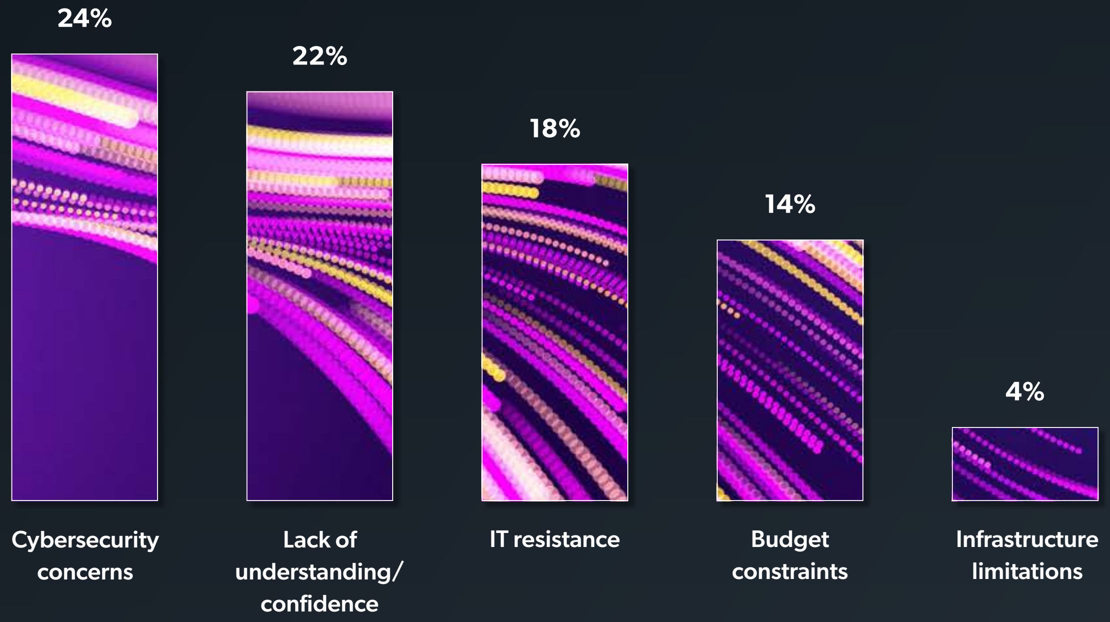
However, for organizations without a cloud strategy, several persistent obstacles remain.

Cybersecurity concerns continue to be the top deterrent, with many End Users still wary of third-party hosting and shared environments. Close behind are confidence and knowledge gaps - nearly a quarter of respondents admit they don't fully understand how to evaluate or deploy cloud solutions securely. Resistance from IT departments, often stemming from control and policy concerns, further slows adoption. Budget constraints and legacy infrastructure complete the picture, hinting that while intent exists, readiness does not.

Together, these barriers suggest the industry's challenge is no longer about proving the value of cloud, but about building the trust and education needed to implement it.

Interestingly, the same forces driving organizations toward cloud adoption - IT alignment and cybersecurity - are also the ones holding many back, highlighting a market still learning how to balance innovation with control.

Cloud detractors



Together, these barriers suggest the industry's challenge is no longer about proving the value of cloud, but about building the trust and education needed to implement it.

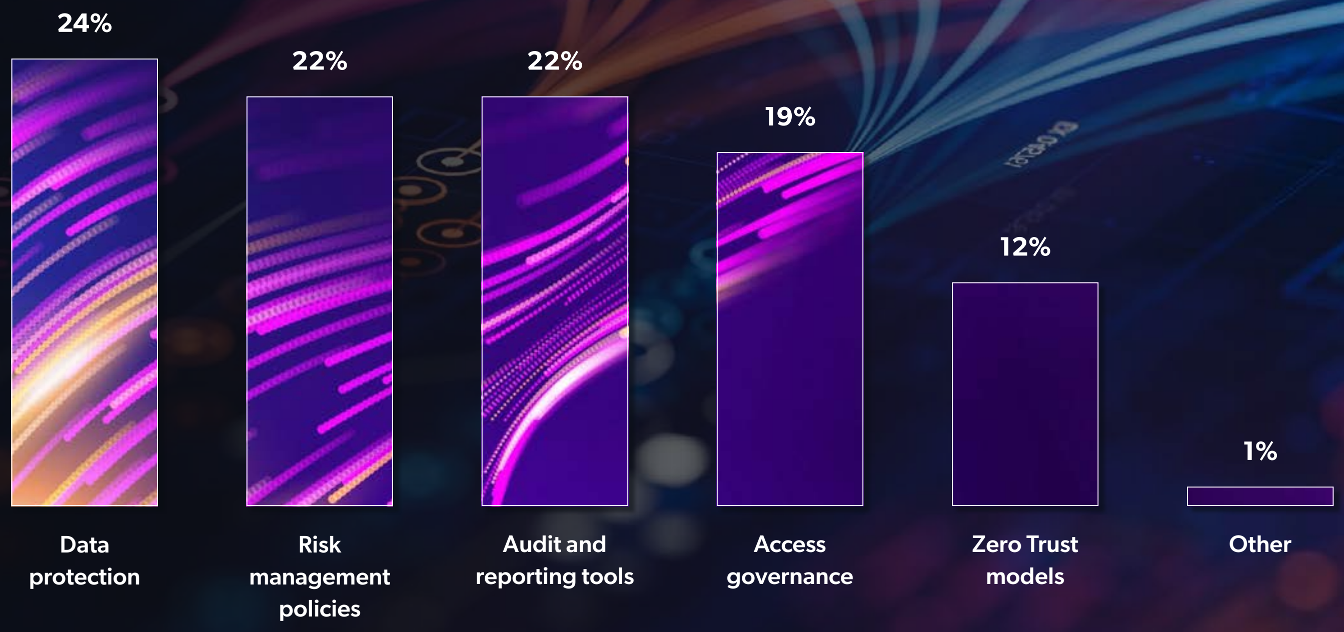
Cybersecurity strategies front of mind

Across the board, cybersecurity remains the most developed strategic area, with 73% of survey participants reporting active frameworks around governance, compliance, and risk.

These results suggest cybersecurity strategies are shifting from reactive protection toward proactive governance. Data protection, risk management, and audit tools lead focus areas, indicating a growing emphasis on formalized policies, accountability, and compliance visibility.

It's important to note, however, that these results may be influenced by the types of vertical markets represented in this year's survey. Most End Users and Channel Partners report servicing highly regulated or security-conscious sectors such as government, education, healthcare, and data centers, industries that inherently demand stronger governance frameworks and typically have greater resources to support them. This context likely contributes to the high percentage of respondents citing formalized cybersecurity strategies and tools as established priorities.

Cybersecurity focuses

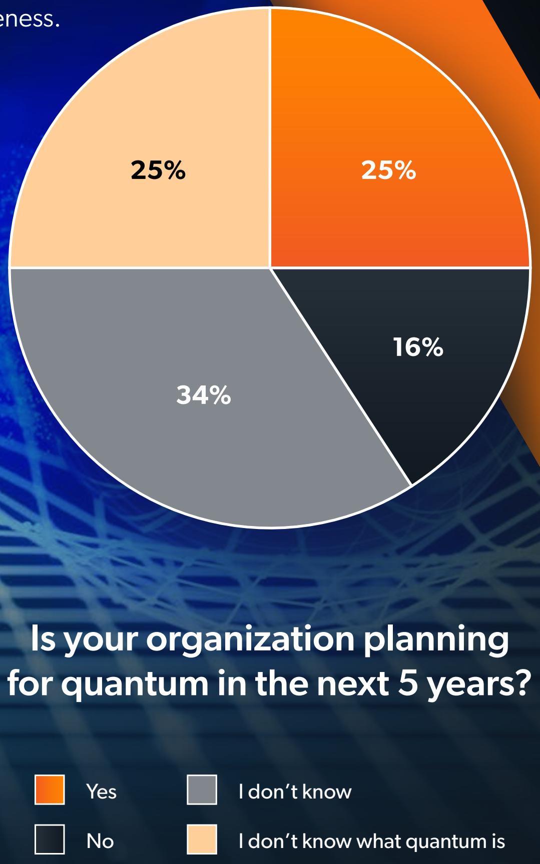


The building case for quantum

Quantum technology is beginning to enter the conversation, though understanding remains limited.

When asked if their organization was considering how security might adapt to or leverage quantum technology in the next five years, responses revealed an industry at the early stages of awareness.

While only one in four survey participants are actively considering quantum, its presence in responses suggests a gradual shift from theory to curiosity, echoing where AI sat just a few years ago.



Is your organization planning for quantum in the next 5 years?

Quantum and the psychology of trust

For decades, security has been defined by doubt. Every process is built to verify, authenticate, and challenge, from confirming individual identity to validating the integrity of our most important institutions. It's a necessary skepticism, but one that has also shaped a culture of caution and constraint.

Quantum technology may quietly begin to change that.

Unlike traditional systems that rely on mathematical complexity to make intrusion improbable, quantum technology removes the rate of probability current algorithms are so heavily reliant on. It invites a new kind of confidence that trust can be known with certainty rather than assumed.

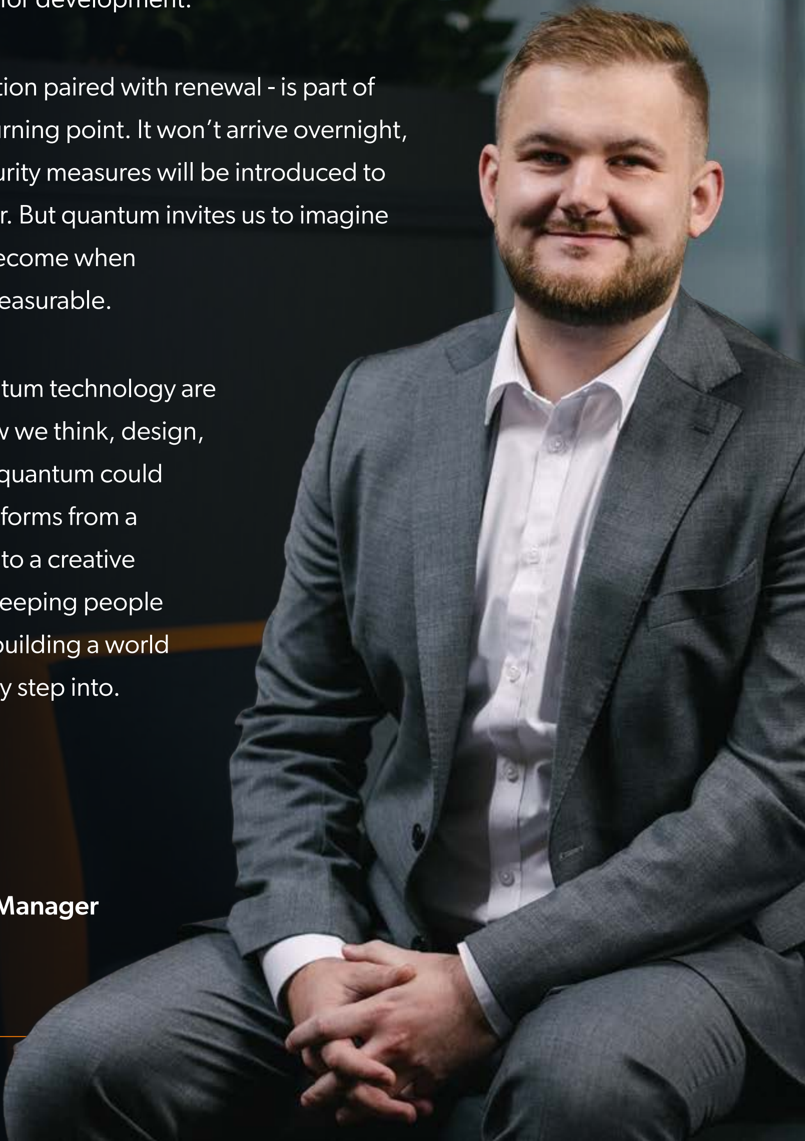
Yet the deeper shift in the short term will be psychological.

Our trust in information has been challenged by artificial intelligence, but quantum may help restore our faith in what's real. In doing so, it'll create a new relationship with truth, where verification becomes an act of assurance rather than suspicion - and that certainty carries as much emotional weight as it does technical value.

However, progress comes with paradox. The same power that makes quantum secure will also test today's encryption standards, demanding new algorithms, frameworks, and mindsets. As a security manufacturer, it's imperative that we continue to secure our products to the highest levels and stay informed of the latest technologies when bleeding edge technology is so close. The path to quantum security starts by adapting systems and processes whilst rebuilding some of the products and platforms relied upon for development.

That tension — disruption paired with renewal - is part of every technological turning point. It won't arrive overnight, and harsher cybersecurity measures will be introduced to lower the attack vector. But quantum invites us to imagine what security could become when trust itself becomes measurable.

The principles of quantum technology are already reshaping how we think, design, and connect. In time, quantum could transform security platforms from a defensive discipline into a creative one that's less about keeping people out, and more about building a world people can confidently step into.



Matt Wills
European Technical Manager

Expanding Value

Security is proving to be much more than protection. It’s driving efficiency, insight, and accountability across organizations, with 35% of Channel Partners and 34% of End Users reporting definitive organizational value derived from their systems.

Surprising business value

Data consistently stood out as the engine driving this expanded value.

Both Channel Partners and End Users emphasized how integrations and APIs are transforming traditional monitoring tools into intelligent business systems capable of delivering insights about occupancy, efficiency, and compliance.

Organizations are using access control data to understand who's on site, how space is being used, and where inefficiencies exist. For some, that means optimizing building performance or automating contractor management; for others, it means strengthening accountability and compliance.

Channel Partners consistently pointed to cost reduction, time savings, and operational efficiency as top selling points to customers. Meanwhile, End Users highlighted human and experiential benefits, like improved accountability, smoother workflows, and better user experiences.

"Reporting features are flushing out staff doing the wrong thing."

"Reporting on contractor hours improved compliance with service agreements."

"Access control data can be used to track employees' check-in and check-out, serving as an automated input for the payroll system."

"By integrating our system with visitor management, VMS, and monitoring station, we're seeing benefits for contractor management."

"Monitoring building occupancy and critical environments has improved space utilization and workplace performance."

"An unexpected benefit is the monitoring of temperature critical environments. There are freezers at our university which contain research; security get notifications in the event of a freezer having temperature issues which prevents lost research."

However, 50% of Channel Partners and 36% of End Users said they don't know if such value is being extracted, suggesting there's still untapped potential waiting to be uncovered – and room for communication improvements to bring Channel across the unexpected benefits their customers are gaining.

"Site security helped renew contracts by increasing staff accountability and reducing theft."

"Our system is used for monitoring and preventing employee access for compliance training."

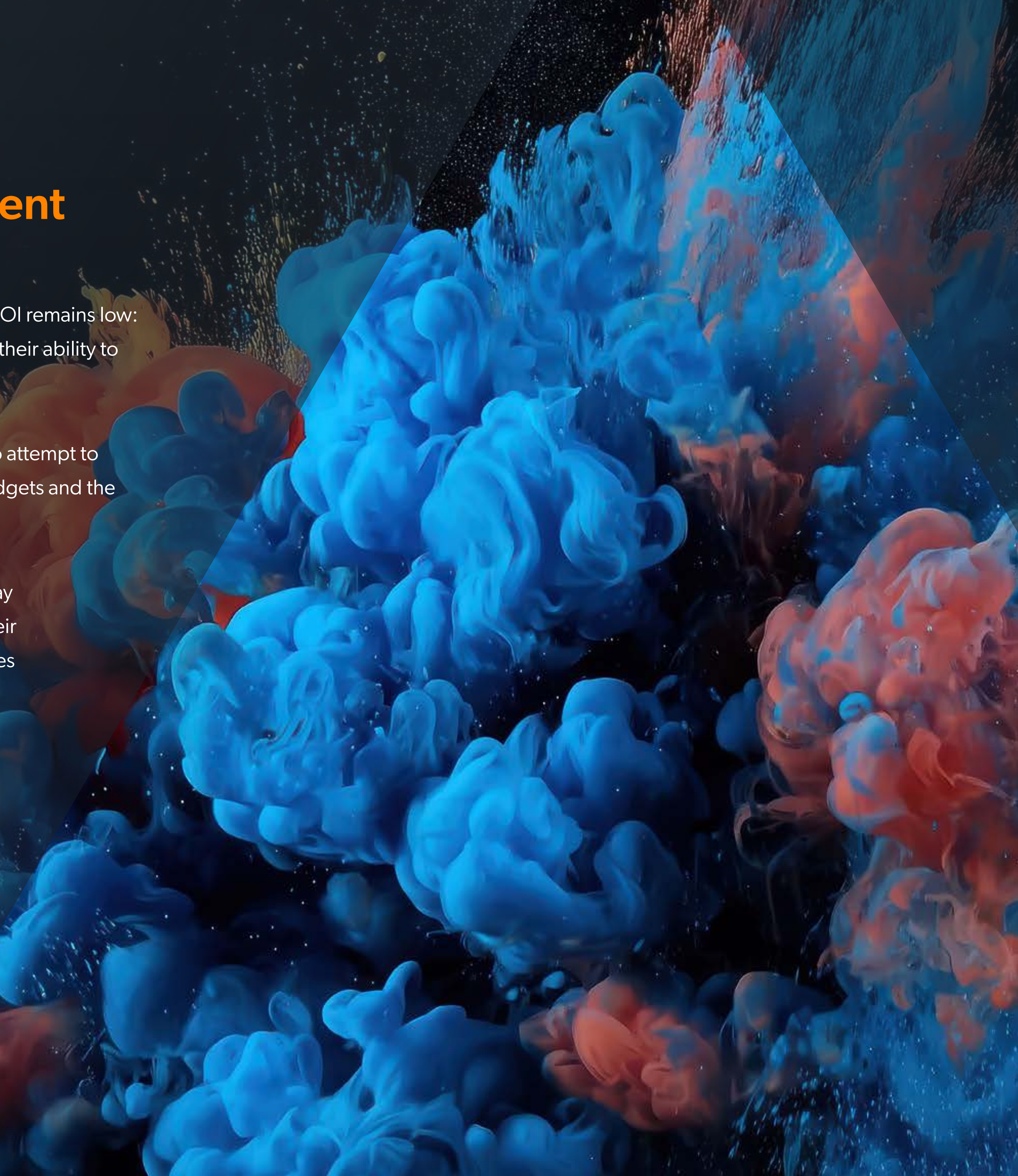
Confidence in ROI measurement

Despite clear evidence of growing value, confidence in measuring ROI remains low: only 32% of all survey respondents said they are "very confident" in their ability to measure the ROI of their security solutions.

Nearly a third of participants either lack confidence or are making no attempt to quantify their system's return, an important gap given tightening budgets and the growing number of stakeholders influencing purchasing decisions.

Channel and Consultant participants appear more proactive: 63% say they're actively helping customers find and apply new value from their systems, compared with 37% of End Users who have formal strategies to do the same. This imbalance highlights an opportunity for the industry to equip End Users with stronger measurement tools and confidence, helping them communicate ROI not only to security leaders, but also to IT, HR, and finance decision-makers.

If the industry can position itself as a value driver rather than a cost center, it could help organizations overcome budget constraints, secure stakeholder buy-in, and accelerate their ability to achieve security goals.



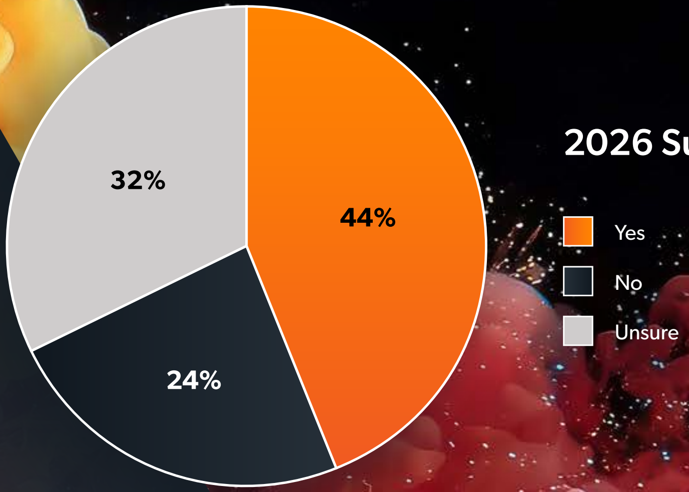
Sustainability strategies slowing

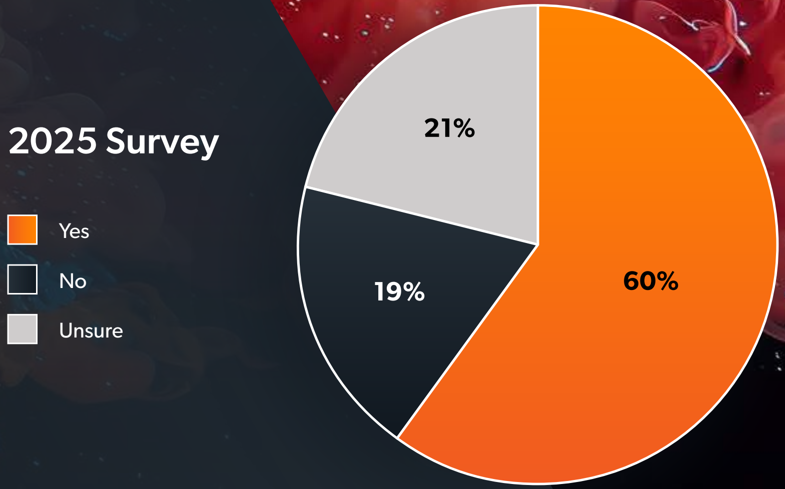
When asked whether their organization has sustainability strategies in place, only 44% of survey participants said yes, marking a significant decline from last year's report, where 60% said they had strategies in place.

In 2025, one-third of those who said they did not have strategies in place expected them to be implemented within six months, but that momentum hasn't materialized. Instead, it appears to have reversed.

This slowdown may reflect a broader global trend. Many organizations have already implemented the most accessible sustainability measures such as energy efficiency or waste reduction, but are now struggling with the cost, complexity, and regulatory uncertainty of scaling their efforts (Jamison, 2024).

Sustainability is also becoming increasingly integrated into "business as usual," which may make some respondents less likely to view these actions as distinct strategies (Jamison, 2024). Combined with tighter budgets, a growing focus on digital transformation, and the need for upgrades, it's unsurprising that fewer organizations report having formal sustainability programs in place.





Security needs a new language for value

In operations, we measure everything, from time to cost, efficiency to outcomes, and everything in between. Yet when it comes to security, assessing the return on investment still eludes many organizations.

That's not because the value isn't there. It's because we're using the wrong lens to quantify it.

For decades, ROI in security was synonymous with loss prevention. But as the systems we deploy have evolved - connecting people, data, and processes - their impact has expanded into areas our old metrics were never designed to capture. Access control data now informs workforce planning. Event logs improve compliance. Analytics shape how we design and use our physical spaces. And so on and so on. These are measurable outcomes, but they don't fit neatly into the traditional formulas.

If we want security to be seen and funded as a value driver, we need to broaden our definition of ROI. That starts with aligning metrics to operational realities: measuring time saved, accountability increased, energy reduced, and confidence gained. It also means improving how we communicate those results to decision-makers beyond the security team, translating technical performance into business outcomes that resonate at every level to ultimately inform capital budget prioritization.

Progress won't come from new tools alone, but from understanding and proving the differences they make across the organization. When we learn to quantify the ripple effects of good security - such as productivity, sustainability, and trust - we close the ROI gap, strengthening our industry's strategic influence and making the business case clearer than ever.

Rachel Wright-St. Clair
Chief Operations Officer

Word on the Ground: Regional Insights

United States

Andriy Tsinyk
Business Development Manager

"In the U.S., there's a growing shift toward cloud-based solutions, particularly as IT professionals take on a greater role in decision-making. At the same time, economic uncertainty and tariffs are driving End Users to be more cautious with spending, seeking solutions that balance cost and value. Channel Partners are increasingly focused on delivering software-as-a-service [SaaS] models that generate recurring monthly revenue and stronger long-term ROI."

LATAM

Luisa Merlano
Technical Solutions Specialist

"The key trend in LATAM is justifying higher investments through deep operational value. We're seeing End Users look past the cost of securing doors and actively using our platform's data and automation tools to improve workflows, reduce non-security costs, and prove a clear return on investment."

United Kingdom

Ian Compton
Sales Manager

"UK organizations are slowly shifting toward cloud-enabled, mobile-friendly access control with greater focus on integration and user experience. While AI and analytics continue to shape discussions, cybersecurity and compliance remain the biggest challenges."

Nordics

Håkan Björkman
Regional Manager

"The Nordic security market is undergoing a clear transformation from traditional, separate technical systems to integrated platforms that are fully part of customers' digital infrastructure. A growing trend is the demand for global system solutions platforms that can manage security needs across multiple geographic markets simultaneously and create unified processes and standards across national borders."

South Africa

Tarryn Fortune
Sales Manager

"Over the past year, conversations with Channel Partners and End Users across South Africa have revealed a clear shift in expectations around security solutions. While technological innovation continues to be a driving force, what's resonating most on the ground is the demand for people-first systems - solutions that are intuitive, adaptable, and deeply integrated into broader operational goals. Businesses are no longer viewing security as a siloed function. Instead, they're leveraging it to support operational efficiency, data-driven decision-making, and even sustainability goals."

Middle East

Nemer Mdardas
Regional Director

"The region is rapidly embracing advanced technologies and SaaS solutions, with government mandates in markets like the UAE and KSA accelerating cloud adoption, AI, and data sovereignty requirements. Security systems are now delivering value beyond protection, as customers use data to drive operational efficiency and cost savings. This shift opens the door for security to evolve from a protective function into a strategic enabler of digital transformation."

Asia

Jin Hui
Regional Manager

As the front-end devices for multi-factor authentication gain popularity, I believe it's becoming increasingly important to focus on the complexity of authentication logic within back-end devices, particularly in high-security environments. I've also observed a significant market shift towards cloud-based solutions, which is increasingly becoming the norm. This transition highlights the importance of effective data transmission and credential management between local systems and cloud infrastructure.

New Zealand

Wayne Scott
General Manager - Sales

In New Zealand, we're seeing a clear trend toward making better use of the data captured by security systems by presenting it to end customers in intuitive, dashboard-style format. We're exploring how AI will change the way we engage with these systems moving forward.

Australia

Keith Neville
Sales Manager

Customers are increasingly seeking to simplify processes and improve business efficiency by maximizing the value of both new and existing technology investments. Achieving this requires strong collaboration among all stakeholders to clearly understand and align on desired outcomes. Effective collaboration throughout the lifecycle is essential to delivering the intended outcomes and ensuring full return on investment and customer satisfaction.

The Next Standard

If there's one message to carry forward from this year's report, it's that the next standard for the security industry won't be set by technology alone. Instead, it will be defined by the intent behind it, and the creativity of the people who choose to use it well.

Every advancement brings both opportunity and responsibility. We have the capability to protect, connect, and understand more than ever before. Our challenge - and opportunity - is to apply that capability with integrity and a shared commitment to creating safer, more sustainable outcomes.

The insights within these pages reflect an industry coming of age. We're beginning to measure progress not only by what we build, but by the impact those efforts have on people, organizations, and the world around us. That shift represents real maturity. It shows how far we've come, from being reactive to change to making the conscious effort to proactively lead the way with clarity and purpose.

Still, the path forward requires all of us. It will take collaboration, curiosity, and a willingness to challenge what's comfortable, because progress happens when insight turns into action, and when innovation serves a greater good.

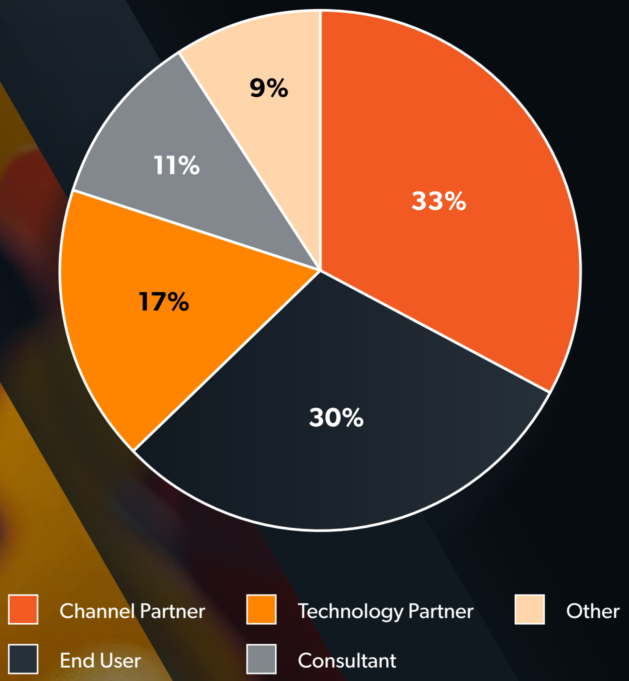
As you look to the year ahead, I hope this report reminds you that the future standard for security is being written right now, through the choices we make, the partnerships we form, and the courage we bring to building what lasts.

Kahl Betham
Chief Executive Officer

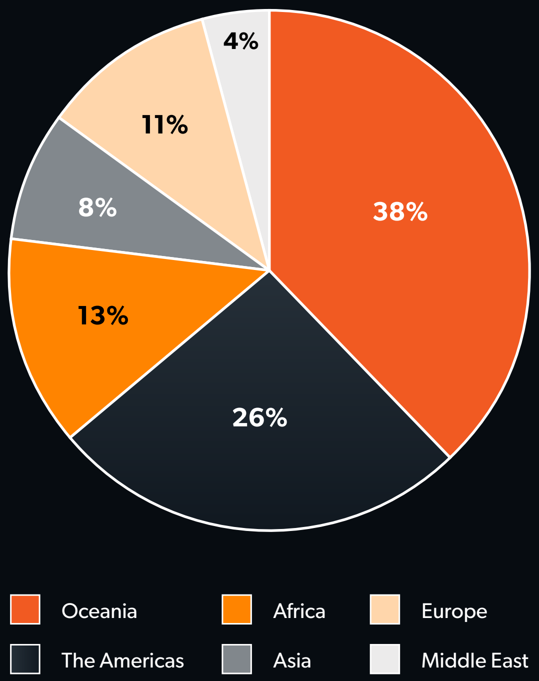
Methodology and Demographics

From August 11 to October 4, 2025, Gallagher Security surveyed global security professionals with the intent of understanding the future of their organizations and what they perceive as the most important issues impacting their security goals in the year ahead. Surveys were distributed across Oceania, the Americas, Europe, Asia, the Middle East, and Africa.

Participant overview



Respondents by region



References

Alaamer, K. (2025, April 22). *This is the state of play in the global data centre gold rush*. World Economic Forum. https://www.weforum.org/stories/2025/04/data-centre-gold-rush-ai/

D'Ambrosio, D., Jacamon, V., Martinos, A., Salmon, N., & Wanner, B. (2025, April). *Energy and AI: World energy outlook special report. International Energy Agency.* https://iea.blob.core.windows.net/assets/601eaec9-ba91-4623-819b-4ded331ec9e8/EnergyandAI.pdf

Data Center Market Size, Share & Industry Analysis, By Component (Hardware, DCIM (Data Center Infrastructure Management) Software, and Services), By Data Center Type (Colocation, Hyperscale, Edge, and Others), By Tier Level (Tier 1 and Tier 2, Tier 3, and Tier 4), By Data Center Size (Small, Medium, and Large), By Industry (BFSI, IT & Telecom, Healthcare, Government, Manufacturing, Retail & E-commerce, and Others), and Regional Forecast, 2025-2032. (2025, September 29). Fortune Business Insights. Retrieved October 17, 2025, from https://www.fortunebusinessinsights.com/data-center-market-109851

Data centres and data transmission networks. (2023, July 11). International Energy Agency. Retrieved October 17, 2025, from https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks

How AI is transforming data centers and ramping up power demand. (2025, August 29). Goldman Sachs. https://www.goldmansachs.com/insights/articles/how-ai-is-transforming-data-centers-and-ramping-up-power-demand

International Monetary Fund. (2025). *World economic outlook: Global economy in flux, prospects remain dim*. Retrieved October 17, 2025, from https://www.imf.org/en/Publications/WEO/Issues/2025/10/14/world-economic-outlook-october-2025

Jamison, S., Macchi, M., Neubauer, M.B., & Moussavi, B. (2024). Destination net zero: Companies are decarbonizing. But how can they go faster? In *Accenture*. https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/Accenture-Destination-Net-Zero-Final-Report.pdf#zoom=40

Lichtenberg, N. (2025, October 7). *Without data centers, GDP growth was 0.1% in the first half of 2025, Harvard economist says*. Fortune. https://fortune.com/2025/10/07/data-centers-gdp-growth-zero-first-half-2025-jason-furman-harvard-economist/

About Gallagher Security

Gallagher Security is a global leader in integrated technology solutions that unlock customer value through the power of our people and products. Our award-winning technology is trusted by government, defense, commercial, industrial, healthcare, transportation, mining, and educational organizations in over 140 countries.

Our team designs and manufactures a comprehensive suite of security software and hardware, including integrated access control, intruder alarm, and perimeter solutions. We're painting the future of what's possible. From making sure people go home safely to their families each night to helping organizations become more efficient, production, and profitable. Security is just the beginning.

Visit security.gallagher.com to learn more

GALLAGH

GALLAGHER™
Security