

Security Industry

TRENDS REPORT

2027

GALLAGHER Security



Author: Rachel Akbar Design: Jason Lurman & Maddison Shaw

Contents

Beyond "What If?" 4
Executive Summary 5
2026 vs. 2027 6
- What's continuing 6
- What's changing 6

Who Owns the Data? 8
- Other industries got here first 9
- Security is buying in 9
- Data collection and the value of control 10

Investment Outlook 11
- Budget outlooks are diverging 12
- Software and analytics lead spending 13
- Automation tops the long view 14
- Executive and finance influence decisions 15
- IT sets the direction 16
- The orphaned estate 17

Shifting Foundations 18
- Integrations top the End User feature list 19
- Governance outranks cybersecurity 21
- Sustainability strategies are widely set 22
- Awareness of quantum computing is growing unevenly 23
- When data becomes intelligence 25

People 26
- Workforce constraints aren't easing up 27
- Training is the universal answer 28
- AI is expected to carry volume, not judgment 29
- Why we still need to be in the room…just better 31

The Burden of Proof 32
- Proof is still scarce, but less than it was 33
- Cloud adoption is outpacing the ability to evaluate it 35
- What we mean when we say "cloud" 37

Word on the Ground: Regional Insights 38
Behind the Badge 41
Methodology and Demographics 42
References 46
About Gallagher Security 47

Beyond "What If?"

For the fourth year in a row, security professionals around the world have come together to help us capture an annual snapshot of our industry. Over the years, this report has tracked security's digital transformation, tested our assumptions, and watched emerging trends take shape.

Along the way, we asked a simple yet powerful question: What if security was capable of so much more than we've previously imagined? This year, some answers are starting to emerge. The industry is moving beyond imagining what might be possible and beginning to put those possibilities into practice.

As we head into 2027, that momentum is carrying us somewhere exciting. This year's report shows an industry becoming more decisive about how new capabilities will be put to work and increasingly focused on what else they can unlock. The question is shifting from "*what if?*" to "*how?*" How do we turn what we've built into greater customer value? And how far can we take it?

Creative problem solving is one of Gallagher's core values, and it feels made for this moment in time. Even when the path forward seems clear, we still find ways to go further.

The next chapter for our industry is ours to shape. I hope this report inspires you to make the most of it.

Mark Junge
Chief Executive



Executive Summary

Although the uncertainty of recent years hasn't dissipated, this year's report shows that organizations have stopped waiting for the discomfort to pass and are instead embracing the industry's new normal. Decisions that were deferred are being made, and commitments are being entered into while the conditions around them are still taking shape.

What's being lost in the movement, however, is any clear answer to who owns the outcome. Security has become a data industry, and organizations are committing faster than they are working out who is answerable for the results. That gap will inform the year ahead.

The industry has stopped waiting

Cloud commitments are up, AI tools are in widespread use, and sustainability strategies are largely in place. What organizations can't yet confidently show is what the return on these investments has delivered.

Investment priorities are shifting

Software upgrades and analytics have displaced hardware at the top of investment priorities. The estate is still physical, but analysis and insights are where organizations see the true value.

Security is absorbing obligations set elsewhere

Governance, compliance, and sustainability requirements are being handed to security teams, even though the obligations originate elsewhere in organizations. What was bought to keep people, sites, and assets safe is now expected to produce evidence for departments that never used it previously.

Ownership is the unanswered question

More functions than ever shape purchasing. IT continues to extend its hold over technical direction, while executive and finance teams have moved ahead of facilities in the buying conversation. However, End Users are less certain than before about who is accountable for the data these systems generate and the risks they carry.

2026 vs. 2027

This year's survey shows an industry whose foundations are holding while ambitions grow. Integrations, budget pressures, and cybersecurity discipline sit where they did a year ago. What's shifting are the tasks organizations want their systems to accomplish, and the answer lies in software, analytics, and automation.

What's continuing

Integrations still define system choice. For the second year running, End Users ranked system integrations as the most important feature when selecting a security system (19%), albeit narrowly ahead of performance and scalability (18%).

Labor outranks budget as the industry's largest challenge. Constrained budgets are the single most frequently named challenge for End Users (27%) and Channel (23%) alike, but staffing shortages and a lack of skilled technicians combined account for more with 32% of End User mentions and 34% of Channel.

Cybersecurity priorities are steady. 76% of participants report active strategies around cybersecurity, governance, or compliance, on par with last year's 73%. The focus hasn't moved either: data protection, risk management policies, audit and reporting tools, access governance, and Zero Trust lead in the same order as 2026.



What's changing

Automation is overtaking integrations as the defining goal. While integrations remain the key driver of End Users' purchasing decisions, automation has become the top goal organizations want to gain from their systems. The two were tied at the top last year; automation has since pulled ahead while integrations slipped to fifth place in the order of priority.

3–5-year goals year on year

	End Users	Channel Partners
Automation	18% → 20% (+2)	15% → 16% (+1)
Integrations	18% → 14% (-4)	19% → 16% (-3)

Software and analytics displace hardware upgrades. Hardware topped End User investment priorities last year; this year, software upgrades rank first and analytics second, pushing hardware to third. Channel Partners report the same reordering for their customers.

Resistance to AI is changing shape. End User AI implementation crossed into the majority, rising from 44% to 62%. Among End Users still holding back, the most common objection is that the benefits aren't clear, ahead of cost and privacy concerns.

Who Owns the Data?

In 2021, The World Bank made the case for a new social contract with rules governing how data is used and who shares the value it produces (World Bank, 2021). Five years on, most industries are still negotiating what that looks like in practice.

Security is one of them. Platforms initially installed to open and close doors now produce continuous accounts of how a building is occupied, when, and by whom, becoming data infrastructure in the process.



Other industries got here first

Security is late to an argument that has already run elsewhere.

Take banking for example. The EU set common rules for payments in 2007 and revised them in 2015, and the market that grew from those rules gave customers the ability to let other providers reach the account data their bank holds ("Payment Services," 2025).

The European Commission now wants to extend that principle beyond payment. Under its proposal, customers would decide who can access their financial data and why, and the firms holding it would have to hand it over ("Framework for Financial Data Access," n.d.). Its explanation for why the wider market moved so slowly is worth noting: solutions developed in the absence of clear rules of the game.

The same is happening with connected products. The EU Data Act, which has applied since September 2025, gives users the right to access the data those products generate and to move it elsewhere ("Data Act Explained," 2025).

In banking, the technology arrived first, and the terms followed. Security is no different.

Security is buying in

None of this is theoretical for security. The clearest movement in this year's survey is toward the systems that generate and interpret data: software and analytics top investment priorities, automation is the leading long-term goal, and cloud strategies are firming up, moving more of that data off premise.

Analytics and automation both depend on data these systems have already collected, and an analytics platform is only as useful as the history it can read.

Ownership is being settled by purchasing decisions, not by anyone deciding it directly.



Data collection and the value of control

Data has always been the quiet asset underpinning security intelligence. Every credential, every door event, every movement is a record of how a location functions day to day. What's changed is how potent that record has become. Generative and agentic AI can now reason over logs that once sat dormant and act on them at scale. Yesterday's archive is today's fuel.

The law is catching up. Under the EU Data Act (Regulation (EU) 2023/2854), customers have the right to access and move the data their connected products generate. It won't be the last regulation of its kind. Openness stopped being a differentiator the day it became a legal floor, but stewardship didn't.

So now, the most pressing question is no longer how much data can be collected, it's how well End Users can control it.

Control leaks at the seams. A reader from one manufacturer passes data to a controller from a second, then to a third party's head-end, then to a fourth's cloud. Every handoff copies the data and hands it to someone new. Accountability blurs, and exposure grows. By the time any of it reaches an AI model, no one can say with confidence where all of it lives, or who has touched it.

The systems worth trusting will be the ones built for control: a clear system of record, known custody at every handoff, one governed path from the edge to the head-end. They also know what to leave alone, keeping the most sensitive streams separate and under the customer's own control.

Advantage won't go to whoever collects the most. It will go to whoever can account for all of it.

David J. Crawford
Product Manager - AI



Investment Outlook

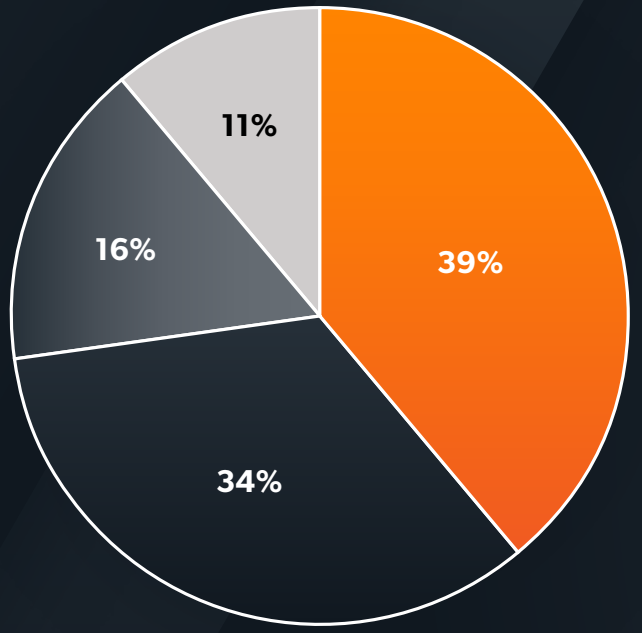
Security budgets are recovering from last year, and how they're being allocated is shifting. Organizations are putting money into software and the analytics layer, while the hardware that once led budgets settles into third place. Value is being sought further up the stack.

This raises a question: when a security investment is weighed, who is actually doing the weighing?

Budget outlooks are diverging

Budget expectations for 2027 show improvement from 2026. A combined 73% of End Users expect their security budget to either increase (39%) or stay the same (34%), an improvement from 66% the year prior.

Channel is moving the other way. 48% expect customer budgets to rise, down from 51% last year, while the share expecting a fall has almost doubled from 8% to 15%. Channel still reads the market more optimistically than End Users do, but its confidence is heading in the opposite direction.



2027 End User Budget Expectations

Increase
Unsure
Stay the same
Decrease

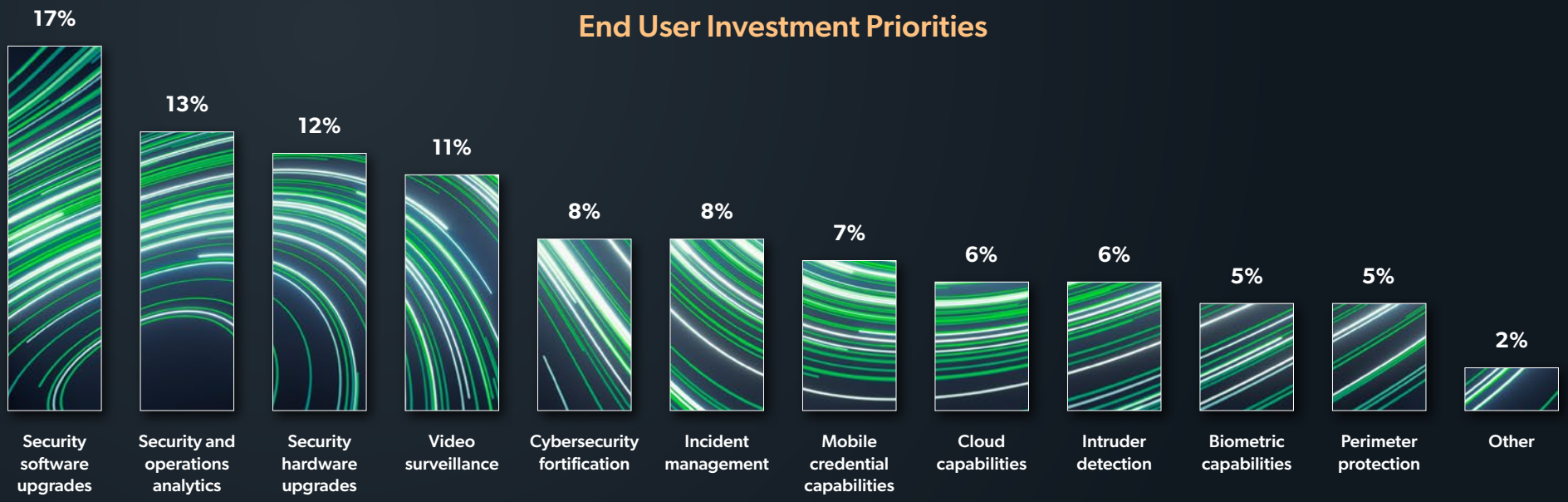
Software and analytics lead spending

Heading into 2027, security software upgrades take the largest share of End User investment mentions at 17%. Security and operations analytics follow at 13%, effectively even with hardware upgrades at 12%.

This marks another shift from 2026, when End Users ranked hardware and software upgrades evenly. This year software has pulled ahead, and analytics has climbed from fourth to second, the largest move on the list.

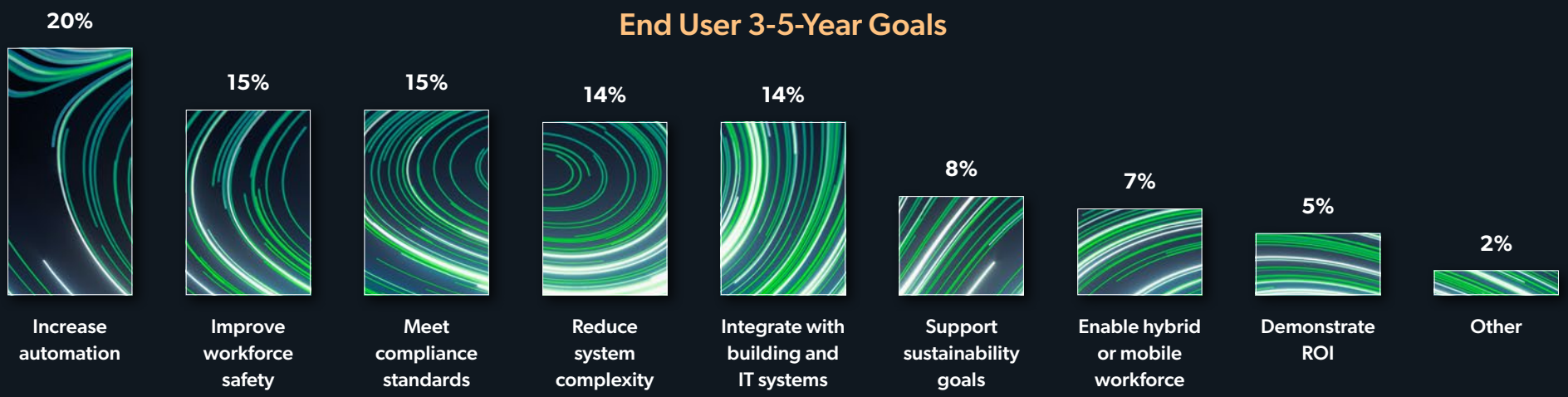
It also follows three years of foundational work. If stabilizing legacy environments is largely accounted for, the next spend lands naturally on the layer above. Investment is following the data rather than the devices that generate it.

End User Investment Priorities



Automation tops the long view

Over a three-to-five-year span, End Users cast a wide net for desired outcomes. Increasing automation takes the largest share of their goal mentions at 20%, comfortably ahead of a tightly grouped second tier: improving workforce safety (15%), meeting compliance standards (15%), reducing system complexity (14%), and integrating with building and IT systems (14%). Channel expects a similar picture, with integrations (16%) and automation (16%) tied at the top and workforce safety fifth at 13%.



In 2026, automation and integrations ranked equally as End Users' top goal. Automation's climb this year - alongside the rise of workforce safety and compliance - points to operational goals displacing security goals and to growing expectations that systems deliver wider business outcomes.

End Users rank return on investment last among the named goals with 5% of mentions. Channel raises it nearly twice as often at 9%. That gap continues from 2026 and is explored further in the report's **The Burden of Proof** section.

Executive and finance influence decisions

Just over half of End Users (53%) report that teams outside security influence purchasing and planning, with Channel reporting the same pattern across its customer base at 60%. Both indicate a continued shift in which teams are in the room.

Among End Users reporting outside influence, the executive team draws the largest share of mentions at 22%, followed closely by finance (20%) and IT (19%). Facilities comes fourth at 17%.

Channel puts IT first and rising, with 27% of mentions this year against last year's 25%. Finance follows at 18%, then executive teams (17%), and facilities (16%).

Facilities' movement is a change worth exploring. A year ago, Channel placed it second, behind only IT. This year, Channel and End Users both rank it fourth. The function that has historically owned building security no longer has the strongest say in what gets bought.

Executive, finance, and IT are all involved, each asking different questions. A proposal built around architecture, integrations, and technical risk likely won't satisfy executive and finance teams asking about cost and business outcome, and increasingly all of them are in the room together.



IT sets the direction

None of this makes IT peripheral, however. On the technical side, it's front and center.

Asked what influenced their cloud deployment decision, End Users put IT strategy ahead of everything else at 29% of mentions - Channel agrees almost exactly, placing IT strategy first at 26%.

IT is just as present in deployment barriers. Among organizations without a cloud strategy, IT resistance is the fourth-named barrier; on mobile wallet credentials, IT limitations rank third among End Users (18%) and fourth for Channel (16%).

That widening remit isn't confined to security. The World Economic Forum's (WEF) Global Cybersecurity Outlook 2026 finds that the convergence of IT, OT, IoT, and robotics now ranks third (42%) among factors organizations weigh in their cyber risk mitigation, behind only geopolitically motivated attacks and disinformation (Moschetta et al., 2026).

The WEF report describes the old separation between IT and operational technology as effectively gone, and governance failing to keep pace. Among organizations with operational technology in their estate, the CISO carries responsibility for both IT and OT in only 36%, one in five maintains a dedicated OT security team, and 16% report OT security issues to the board (Moschetta et al., 2026, p. 36).

IT is absorbing a wider remit than the structures around it were designed to govern, a plausible reason why this report's data shows it as both the leading driver of deployment and a consistent source of friction.

The orphaned estate

Traditionally, physical security has been treated as a building material. It arrived with the fit-out, was expected to last twenty years, and, once commissioned, was largely left alone. That made sense when a lock was a lock, but the door controller is now a networked computer with an operating system, firmware, credentials, and an address of its own.

So why does so much of that estate still have no owner?

Walk through any organization and every other layer of technology has one. The network has an owner. The data platform has an owner. Even each building has its own owner.

And yet, the security estate does not. The controllers, readers, servers, and integrations accumulated site-by-site over twenty years belong to nobody in particular. It was run like plumbing: attended to when it broke, but invisible otherwise. Each individual project had its owner, but the whole wound up orphaned.

Each of those decisions was right at the time. What they added up to is no longer fit for purpose.

When facilities bought for their buildings and integrators delivered on tenders, IT was rarely in the room because the door was not yet their problem. Every decision was made in isolation, resulting in an estate with no architecture, duplicated systems, unmanaged credentials, and risks that never surfaced on dashboards. Many will cite IT's influence on projects, but influence is not ownership.

To close that gap, organizations must treat physical security as a platform with a roadmap, standards, and a named owner, and be held to the same level of discipline as every other layer of infrastructure. The market has reached the same verdict: when a global consultancy pays over $4 billion USD for firms that secure operational devices, it's pricing the door controller as enterprise IT infrastructure (Hollingworth, 2026).

In most cases, the natural owner already exists. The CIO holds identity, data, and integrations.

The estate is already theirs. It's just waiting to be claimed.



Tim Orr
Sales Manager - NZ

Shifting Foundations

Security systems installed today may still be running in a decade, but their obligations will differ from what they were originally specified for.

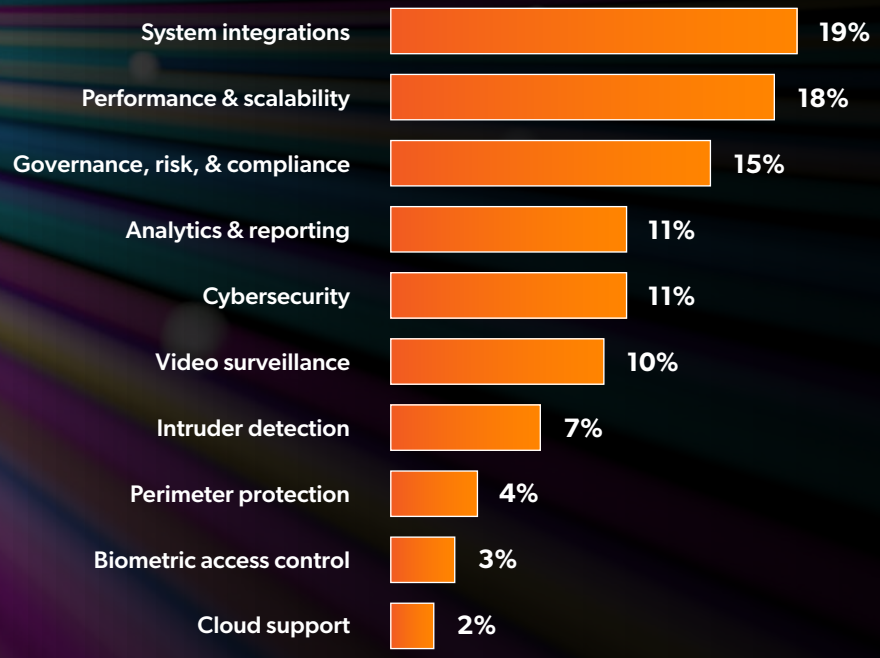
That's the quiet problem beneath today's industry. The list of expectations keeps growing, and less of it comes from security teams. Integrations, compliance, sustainability, post-quantum readiness - each arrives from somewhere else in an organization, on someone else's timeline.



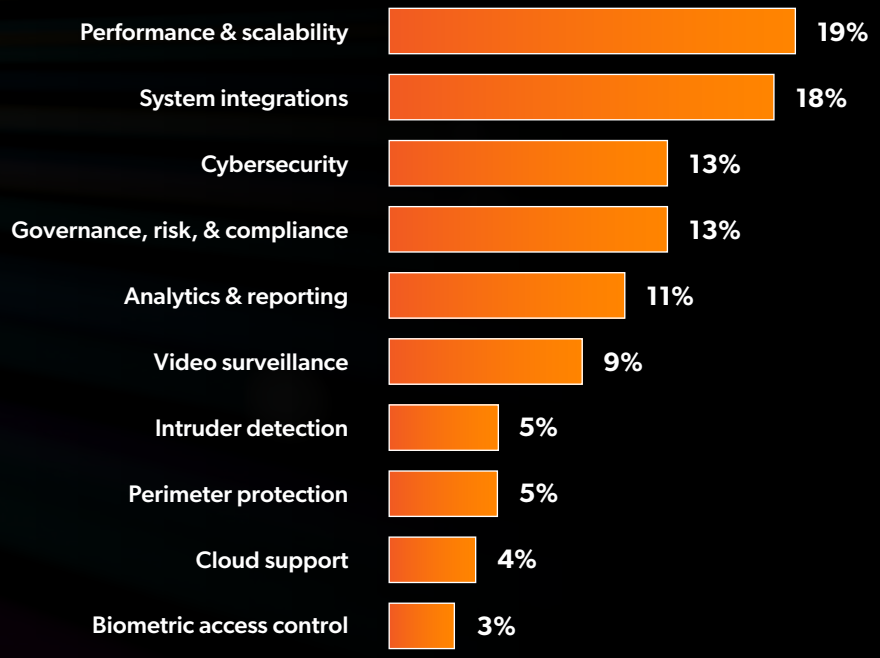
Integrations top the End User feature list

When asked which system features matter most to their organization, End Users ranked system integrations at the top of their list with 19% of mentions. Channel Partners and Consultants placed it second (18%), just behind performance and scalability (19%). Among End Users, performance and scalability climbed from seventh to second, while video surveillance fell from second to sixth.

End Users' Most Important System Features



Channel's Most Important System Features

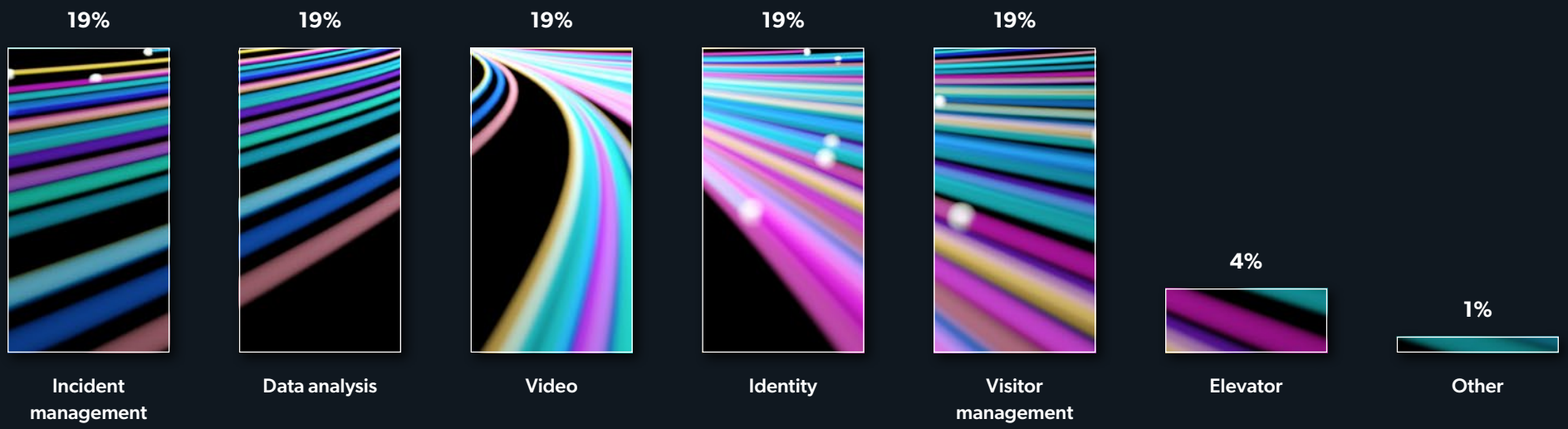


Asked to name their three most important integrations, End Users could not narrow the field. Incident management, data analysis, video, identity, and visitor management each took 19% of mentions, with only four mentions separating first from fifth. That spread reflects how much security is now expected to orchestrate, moving "single pane of glass" views out of nice-to-have territory and into a standing expectation.

Two movements sit beneath that tie. Data analysis has climbed from fifth to joint second, the largest shift of any integration this year, while video has lost the top position it held last year.

Channel's integration priorities are less evenly spread. Video continues to lead at 21%, followed by incident management (20%), identity (18%), visitor management (17%), and data analysis (16%). Video's share has fallen from 26% and data analysis has risen from 10%, so the same two movements are underway in the installation space, though from a wider starting gap.

End Users' Top Integrations



Governance outranks cybersecurity

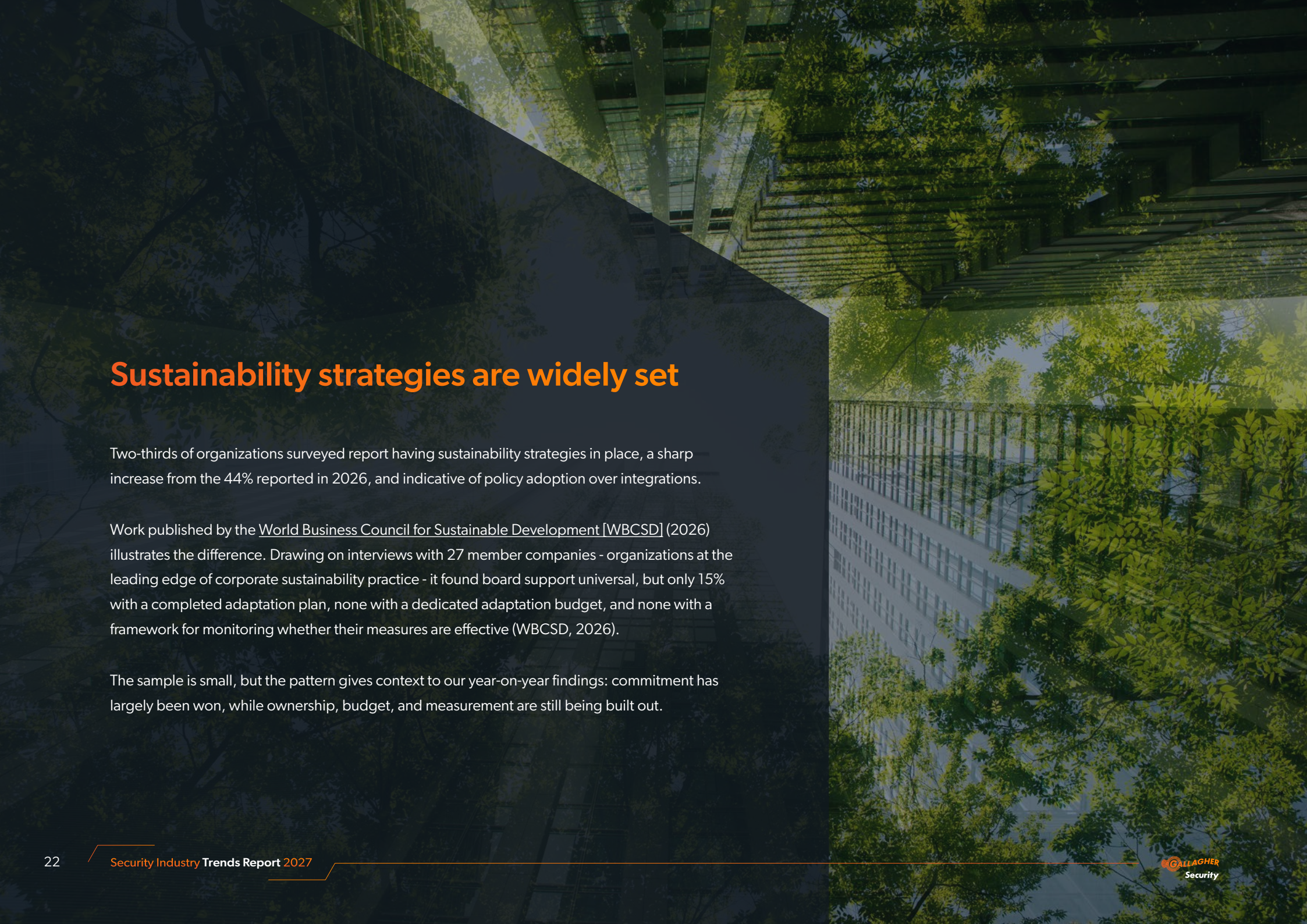
End Users rank governance, risk, and compliance third among the features that matter most, at 15% of mentions. Cybersecurity sits fifth at 11% behind analytics and reporting.

Three years ago, governance failed to crack the top five, and organizations reported their cybersecurity policies were in transition. Both ranking highly now is another indication of security's increasing presence within legal, executive, IT, and broader organizational functions.

Evidence from the wider cybersecurity field suggests why. The WEF's Global Cybersecurity Outlook 2026 found that board members carry personal liability for breaches at 30% of the organizations it classifies as highly resilient, against 9% of those with insufficient resilience. In those same organizations, the security function is involved in the business's wider procurement at 76%, compared with 53% (Moschetta et al., 2026, p. 39).

Where End User organizations have cybersecurity strategies in place, the same priorities lead in the same order as last year: data protection (25%), risk management (22%), audit and reporting tools (21%), access governance (20%), and Zero Trust (11%). Channel is closely aligned at 25%, 23%, 20%, 19%, and 13% respectively.





Sustainability strategies are widely set

Two-thirds of organizations surveyed report having sustainability strategies in place, a sharp increase from the 44% reported in 2026, and indicative of policy adoption over integrations.

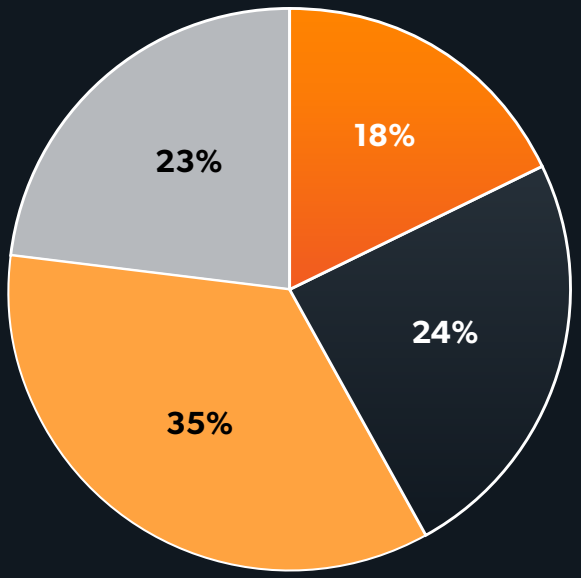
Work published by the World Business Council for Sustainable Development [WBCSD] (2026) illustrates the difference. Drawing on interviews with 27 member companies - organizations at the leading edge of corporate sustainability practice - it found board support universal, but only 15% with a completed adaptation plan, none with a dedicated adaptation budget, and none with a framework for monitoring whether their measures are effective (WBCSD, 2026).

The sample is small, but the pattern gives context to our year-on-year findings: commitment has largely been won, while ownership, budget, and measurement are still being built out.

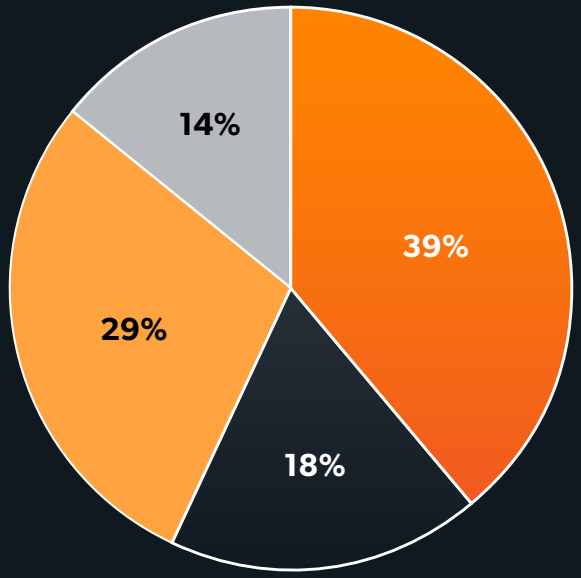
Awareness of quantum computing is growing unevenly

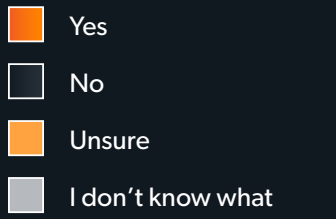
Organizations were asked whether they're considering how their security system might be optimized by quantum computing over the next five years. 18% of End Users said yes, compared with 17% a year ago. Channel reports far more activity, with 39% saying the majority of their customers are considering it, up from 27%.

End Users Considering Quantum Computing Optimization



Channel Considering Quantum Computing Optimization





The responses beyond 'yes' tell a fuller story. Among End Users, 35% are unsure, 24% say no, and 23% report that they don't know what quantum computing is. Channel is more confident overall, but 14% also don't understand the concept. All in all, awareness is greater with the companies that sell and specify security technology, but most End User organizations have not yet formed a view.

Critically, awareness may not be enough in 2027. The WEF found that 37% of industry leaders expect quantum technologies to affect cybersecurity within the coming year (Moschetta et al., 2026, p. 55). As the 2024 post-quantum cryptography standards published by NIST take hold (Boutin, 2024), the WEF warns that "the window for proactive migration to these new cryptographic standards is closing fast," and that by 2030 the greatest systemic exposure will come from legacy encryption (Moschetta et al., 2026, p. 55).

Our survey asked whether quantum computing might improve security systems. The harder question is whether those systems can withstand it, and close to a quarter of End Users don't yet know enough about the technology to consider it.



When data becomes intelligence

When the security industry talks about building smarter systems, the conversation often centers on artificial intelligence. AI deserves its place in the spotlight, but intelligence is about far more than one single technology.

True intelligence is created when people, processes, data, automation, and technology work together to improve decision-making. AI can help with acceleration, but it's only one component of a much larger ecosystem. Today's security environments generate an enormous volume of information. The challenge is turning that information into actionable insight.

When an alarm is triggered, operators must still assess what happened, locate relevant video, match activity across multiple systems, and determine an appropriate response. The data exists, but understanding the event requires manually connecting information across multiple interfaces, consuming valuable time when seconds matter.

Now imagine that process happening automatically. An alarm arrives enriched with the relevant video, access records, sensor activity, and related events, presenting operators with a clear picture of the situation from the start. Time is no longer spent collecting information; instead, operators can focus on action.

That's what interoperability should look like. Not just systems exchanging data, but working together to transform disconnected information into actionable intelligence to make faster, more informed decisions.

Achieving that level of intelligence requires organizations - not vendors - to control how information flows across their security ecosystem. Data locked within systems can be stored, analyzed, and reported on, but its value is limited when it cannot easily connect with information from other platforms. The most powerful insights emerge when data can move freely and create a complete operational picture.

Because in the end, the future of security isn't defined by how much data we collect or how many AI tools we deploy. It's defined by how effectively we transform information into understanding, and understanding into action.

Mariah Rimbert
Business Development Manager - Federal & Commercial - US



People

Since 2024, we've tracked a trend of more demand on security systems: more integrations, more compliance, more automation.

All of it lands on the people who specify, install, service, and operate those systems, and there are not enough of them.





Workforce constraints aren't easing up

Combined, staffing shortages and a lack of skilled technicians makes labor the largest challenge category across the industry, with 32% of End User mentions and 34% of Channel, against budget constraints at 27% and 23%.

Labor was the biggest challenge for Channel in our last three reports as well, with participants specifically calling out "lack of manpower," "keeping workforce skills current," and "turnover of staff and contractors" as top obstacles, regardless of an organization's size, scope, or industry.

In short, labor constraints haven't changed. What *has* changed is what organizations are doing about it.

Training is the universal answer

To address staffing and skills gaps, both groups name training and upskilling well ahead of any other tactic, at 42% of End User mentions and 41% of Channel. However, beyond this, responses diverge.

End Users turn next to automation (19%), then manufacturer-led training and diversifying hiring practices at 11% each. Channel reaches for manufacturer-led training (18%) and more diverse hiring practices (16%), with automation close behind at 15%. End Users appear to be trying to reduce reliance on higher skill sets while Channel is still trying to find more of them.

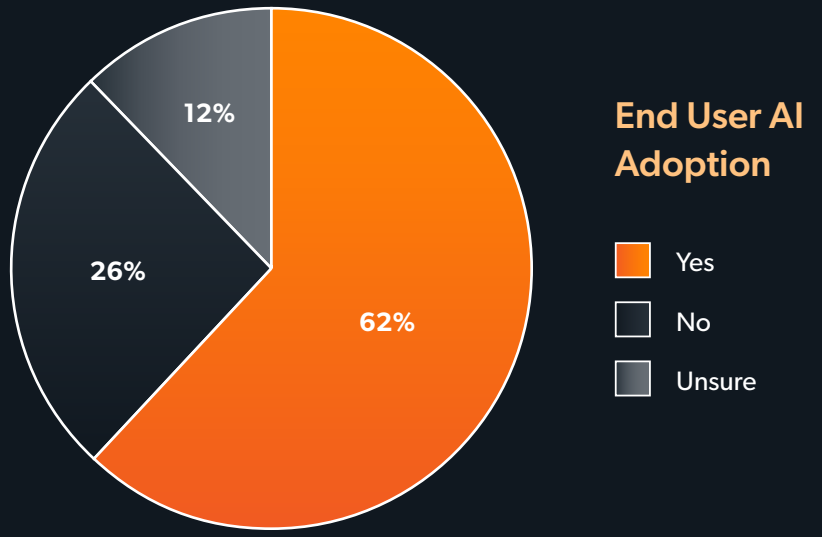
Notably, 14% of End Users report not currently addressing the labor gap at all.

Our 2024 report anticipated part of this, suggesting labor scarcity might push the market toward cloud, which is perceived as easier to maintain, troubleshoot, and upgrade. Organizations are turning to cloud to reduce system demands on their people, but automation has emerged as the preferred answer to this problem.

AI is expected to carry volume, not judgment

62% of End Users report that their organization implemented AI tools or integrations in the past year, up from 44%. Channel observes less adoption, with 40% saying the majority of their customers have made AI headway.

What organizations want from AI is narrower still. Write-in responses describe a consistent division of labor. AI is expected to absorb volume, such as sorting through video footage, triaging alerts, reducing false alarms, automating reporting, and handling repetitive tasks. However, judgment is expected to stay with people. Participants describe AI advising while humans decide, with oversight as non-negotiable. One put it plainly: "AI is not as good as boots on the ground."





Several participants describe AI as creating new skill requirements rather than removing them. A system has to be trained on the specific site it protects along with governance rules, which takes a person who understands both to set up. Once it's running, the operator's job changes from watching screens to judging whether what the system has flagged is real. Both tasks ask for more judgment than the work they replace.

A smaller group remains wary, naming disclosure liability, compliance risk, and the possibility of AI miscalculations as the main barriers to adoption. However, these participants are not necessarily arguing that the technology will fail; they want governance and human oversight established before AI takes on more security functions, which is the same condition the wider group attaches to the uses it already welcomes.

Why we still need to be in the room…just better

ACS26 NEW ZEALAND

We often talk about how our industry needs to modernize and innovate, but that conversation almost always points exclusively to technology and product. It should also point to how we tell stories, how we market and brand, and what we expect from events, including how the information generated at these gatherings reaches outside the physical security industry.

It's time to "show and tell" properly.

Ideas are no longer spread only through PowerPoint decks, lunch-and-learns, and trade show booths. They spread through highly curated and purposeful rooms built for omnichannel conversations. However, most of what we currently have is repurposed packaging of yesterday's experiences, as though we lack the creativity or imagination to evolve.

The Access Control Summit (ACS) exists because events that put those dynamic conversations front and center didn't exist. ACS won't be the only one to reimagine how we come together as an industry. We'll continue to see more, but we need to move faster in this direction.

ACS26 celebrated its 4th year in a country outside the usual circuit, New Zealand, co-hosted with Gallagher Security. The theme, "Our Mainstream Moment," is a statement that access control has outgrown its echo chamber and warrants a wider global audience. We're moving from a cottage industry to a mainstream one and need to hear more from the voices leading this evolution.

The format is built for just that: an in-person discussion paired with content before, during, and after, so the conversation doesn't evaporate when the room empties. This single-day show will give us eight months of stories to tell our core market, but more importantly, to share with the adjacent and mainstream audiences who will make our industry boom.

It's time to build more productive gatherings. If we don't, who will? No better angles are coming, and those who prioritize change and experimentation will reap the rewards.

Lee Odess & Hilary Gallagher

CEO - The Access Control Collective

Chief Operating and Marketing Officer - The Access Control Collective



The Burden of Proof

Most of the shifts this year's report has described raise a similar question: whether security investments can demonstrate their value and return.

This section addresses how rarely that question can be answered, and where opportunities lie to raise security's profile within an organization.



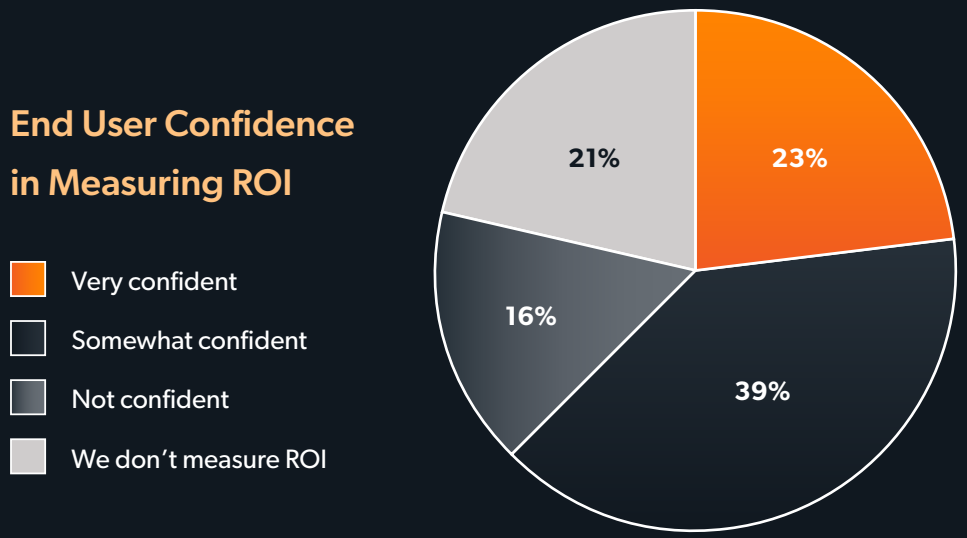


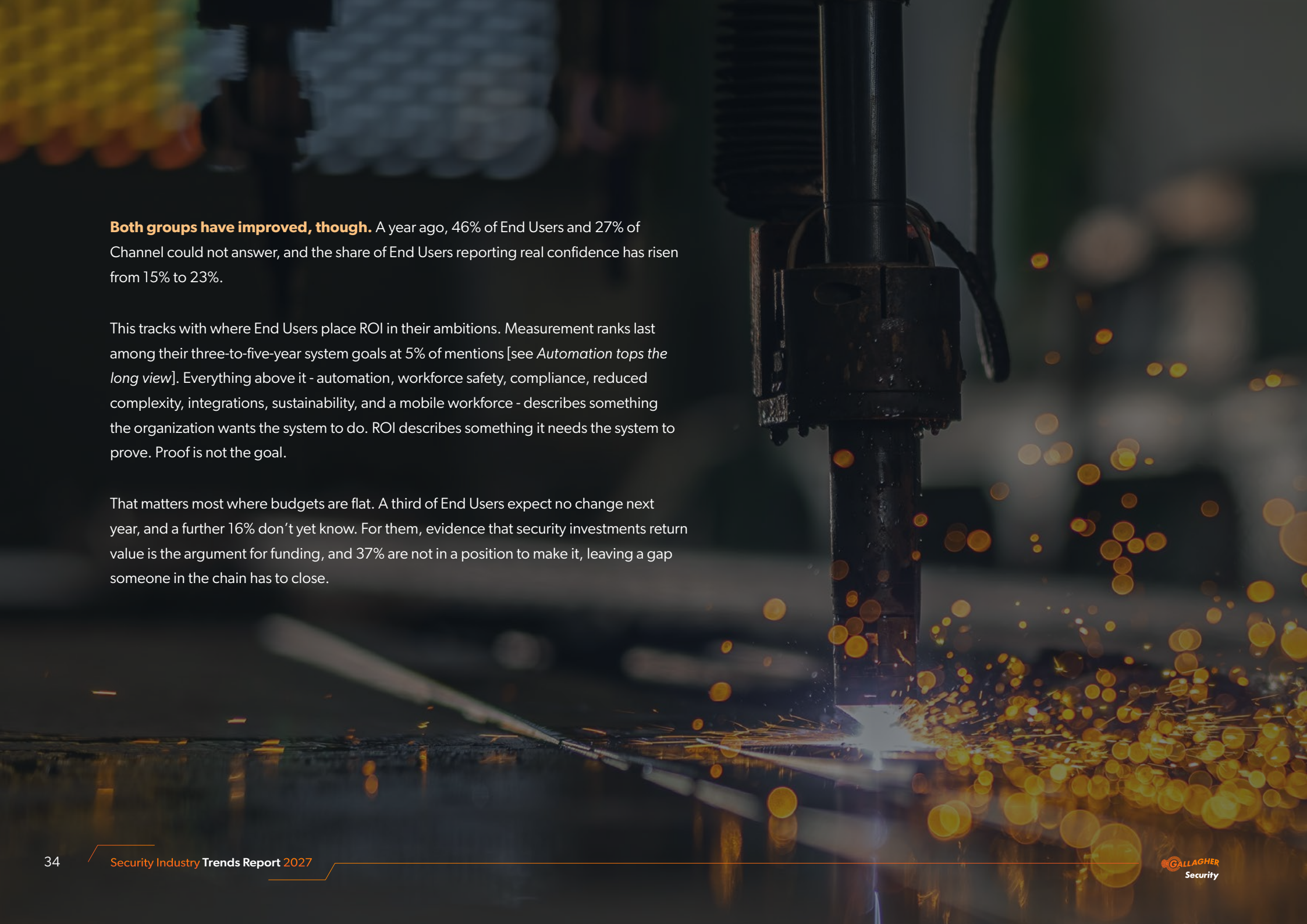
Proof is still scarce, but less than it was

Asked how confident their organization is in measuring the ROI of their system, 44% of Channel Partners say very confident. Among End Users, the figure is 23%.

A further 21% of End Users don't measure ROI at all, and 16% lack confidence in the measurements they have. Taken together, 37% cannot answer the question executive and finance teams are likely to ask. Among Channel Partners, the equivalent figure is 19%.

End User Confidence in Measuring ROI





Both groups have improved, though. A year ago, 46% of End Users and 27% of Channel could not answer, and the share of End Users reporting real confidence has risen from 15% to 23%.

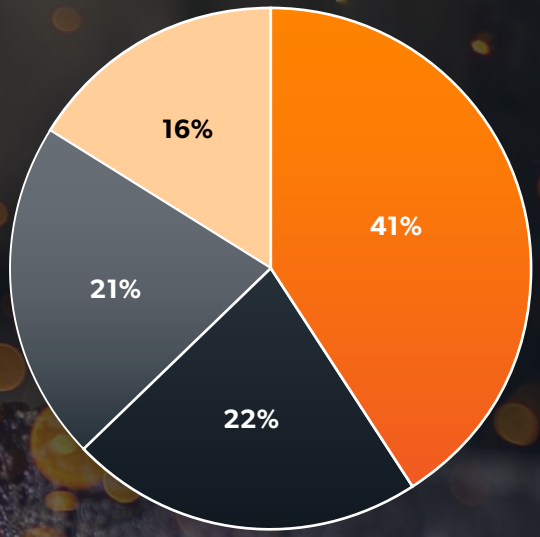
This tracks with where End Users place ROI in their ambitions. Measurement ranks last among their three-to-five-year system goals at 5% of mentions [see *Automation tops the long view*]. Everything above it - automation, workforce safety, compliance, reduced complexity, integrations, sustainability, and a mobile workforce - describes something the organization wants the system to do. ROI describes something it needs the system to prove. Proof is not the goal.

That matters most where budgets are flat. A third of End Users expect no change next year, and a further 16% don't yet know. For them, evidence that security investments return value is the argument for funding, and 37% are not in a position to make it, leaving a gap someone in the chain has to close.

Cloud adoption is outpacing the ability to evaluate it

More organizations are committing to cloud. 41% of End Users have a cloud deployment strategy with a further 16% building one, up from 35% and 12% in 2026.

Channel reports the same shift: 32% of their customers now have a strategy, up from 21%, with a further 22% in development.

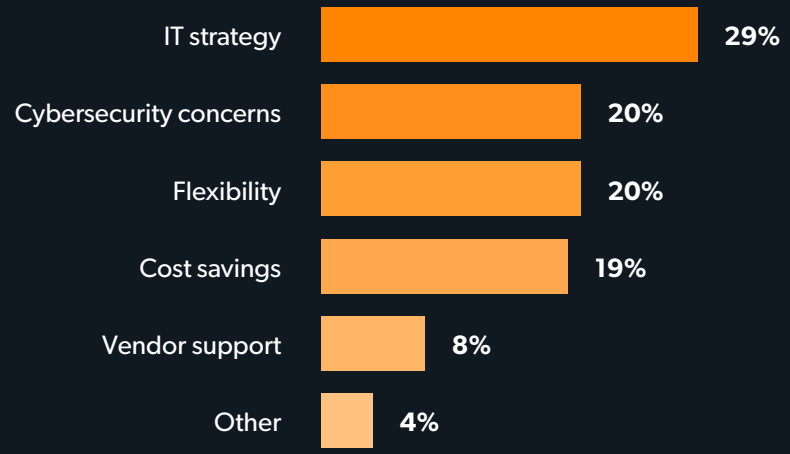


End Users with Cloud Strategies

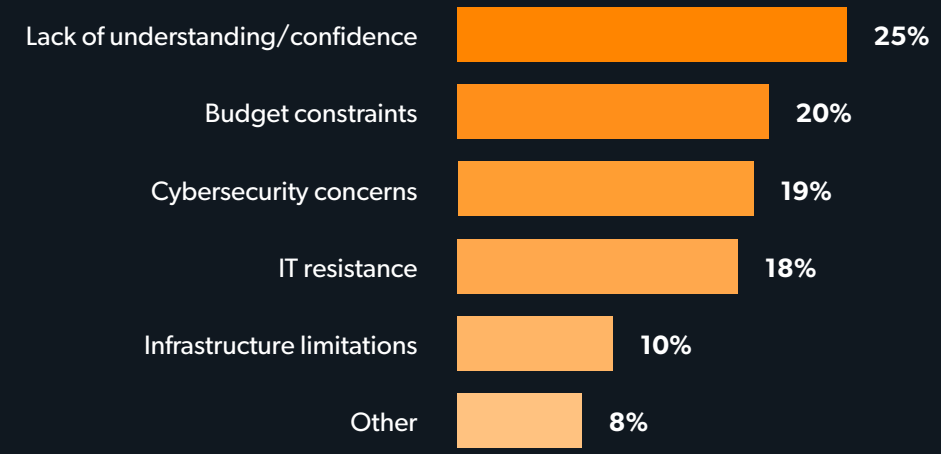
- Yes
- No
- Unsure
- In development

Uncertainty is falling, too. The share of End Users who cannot say whether their organization has a cloud strategy has dropped from 35% to 21%. However, a further 22% report no cloud strategy at all, most often citing a lack of understanding or confidence to proceed as the key barrier. Budget constraints come next, then cybersecurity concerns.

End User Cloud Drivers



End User Cloud Barriers



Write-in responses show an additional barrier. Some organizations are not permitted to use cloud at all, citing compliance rules that require data to stay on premise, data sovereignty, federal certification, local government restrictions, and internal policy as barriers. These organizations have not weighed cloud and rejected it; they were never allowed to weigh it in the first place.

Among organizations that *have* adopted cloud, Channel ranks cost savings second while End Users rank it fourth, a gap worth watching for what it says about appetite for SaaS models and how on-premises costs are perceived.

What we mean when we say “cloud”

Not long ago, an End User told me their access control system was cloud based, and they were right. I heard the same sentiment a week or so later from someone with very different system architecture and needs, and they were right as well.

That’s roughly where our industry sits. The word “cloud” has stretched to cover an enormous amount of ground. Cloud-ready, cloud-hosted, cloud-native, hybrid, SaaS - all in daily use, all understood slightly differently depending on who’s in the room. In other words, when we talk about cloud, we’re all speaking a different language.

The distinction that matters most in practice tends to be the one that gets skipped. When an organization says it wants SaaS, what it frequently wants is a managed service, without major hardware investments, lengthy deployments, and somebody else responsible for keeping the system running. Plenty of hosted arrangements deliver exactly that, and they remain a different proposition from software as a service. Establishing which one is genuinely needed takes a single conversation, and it changes what belongs in a specification.

This matters most at the enterprise level, where the breadth of capability available varies considerably depending on the route taken. The fair question for anyone specifying a system is what they’re choosing to go without, and whether they would miss it. That picture is changing quickly, and much of what sits outside reach today will not stay there.

Both End Users I mentioned had systems that suited them well. Neither, I suspect, would have recognized the other’s from the description.

Gordon Swallow
Regional Business Development Manager - UK/EU



Word on the Ground: Regional Insights

Australia

Jake Kearns,
National Key Accounts Leader

One trend we're consistently seeing across Australia is the increasing demand for unified, scalable security ecosystems that can deliver both operational efficiency and stronger business outcomes. Customers are looking beyond individual products and are prioritising solutions that integrate seamlessly with existing technology investments, reduce complexity, and provide greater visibility across their operations.

New Zealand

Josh Weber,
Technical Account Manager – Lower North Island & South Island

Increasingly I see End Users wanting more out of their systems. Instead of just opening and closing doors, they see opportunities to create an ecosystem that enables them to use their buildings, infrastructure, and processes more efficiently, freeing up their people from repetitive, administrative-heavy tasks and allowing them to work in more impactful and engaging ways.

Asia

Joe Fan,
Regional Marketing Manager

Asia's rapid cloud and AI expansion is driving an unprecedented data center boom across the region. As colocation facilities scale, physical security must evolve beyond simple access control to encompass complete site protection from perimeter fencing down to server rack locking. Unifying these layers on a single high-assurance platform delivers total auditability, seamless compliance, and tenant trust, turning physical security into a core operational asset.



Africa

Tiisetso Khanye, Technical Customer Success Manager

Although system integrators and consultants continue to bridge the gap between best practice and practical implementation, End Users are becoming increasingly self-reliant at managing and accounting for their organizational security requirements. At the same time, there's a growing shift towards ICT-style policies for the ongoing maintenance and management of security systems, driven by the pace of cybersecurity developments and increased awareness of associated risks.

Middle East

Khodor Habbouche, Regional Sales Director

Across the region, the expansion of AI, smart infrastructure, and connected environments is changing how organizations think about security. The market is shifting from standalone security systems towards integrated, data-driven platforms that combine physical security, cybersecurity, and operational intelligence to protect increasingly critical digital and physical infrastructure to face today's challenges.

United States

Eli Pacheco, Senior Technical Support Engineer

We're seeing more organizations migrate to cloud-hosted infrastructure to reduce hardware costs and simplify management. Many sites have historically preferred keeping systems on-premises, but rising server and maintenance costs are driving cloud adoption. At the same time, End Users are increasingly looking for solutions that allow them to manage and maintain their own environments without relying heavily on Channel Partners for day-to-day operations while still leveraging automation, stronger security, and seamless integrations.

Europe

Matt Wills, European Technical Manager

European organisations are increasingly considering protection against emerging technology breakthroughs in their purchasing decisions. National technical authorities are clearly communicating the need for readiness through initiatives such as post-quantum cryptography and AI vulnerability tools, shaping how buyers prioritise investment in security technologies across all sectors.

United Kingdom & Ireland

Jason Hunter, High Security Manager

With the consistent and increased threat from Russia, Iran, and China, more End Users are focused on cyber resilience across their entire estate. The insider threat is still as prevalent as always and is as much of a concern with the UK being a major target to state actors. Manufacturers are waking up to NPSA standards that are available, and more and more are ensuring their equipment has been tested to the highest government standards.



Behind the Badge

Right now, someone is tapping through a turnstile, calling a lift, booking a room, and turning on the lights by walking through a door. One credential, four systems. Ask them how it worked and they'll hold up a badge (or these days, a phone or watch). As far as they're concerned, the badge is the whole thing.

They're wrong, and that's the achievement. Our industry has become very good at hiding complexity, and this year's report shows how far we've taken it. The complexity is invisible to the people walking through the door. That's design working.

But notice what else is invisible. Security that works produces nothing to look at. No incident. No queue. No call to the service desk. The better it gets, the less there is to point at. You can't point at the incident that didn't happen.

That second invisibility is why ownership is an open question in this report. More people than ever shape these decisions, and fewer of them are certain who is responsible for the outcome. And no one wants to take ownership if the value is also invisible.

Ownership really needs to go beyond just taking responsibility for keeping the system maintained. The bigger opportunity is what else the investment can do - new integrations, automations, better reporting, space utilization and beyond. That's how the value stops being invisible.

So the question for next year isn't how much more we can hide. It's what we're prepared to claim. Say what a system is expected to deliver. Write the assumptions down. Then go back and check whether it did.

When security works, nobody notices what's behind the badge. Whoever owns it should.

Josh Arnold
Chief Product Officer



Methodology and Demographics

From June 1 to July 31, 2026, 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 Australia, New Zealand, the Americas, Europe, Asia, the Middle East, India, and Africa. In total, 677 people took part.

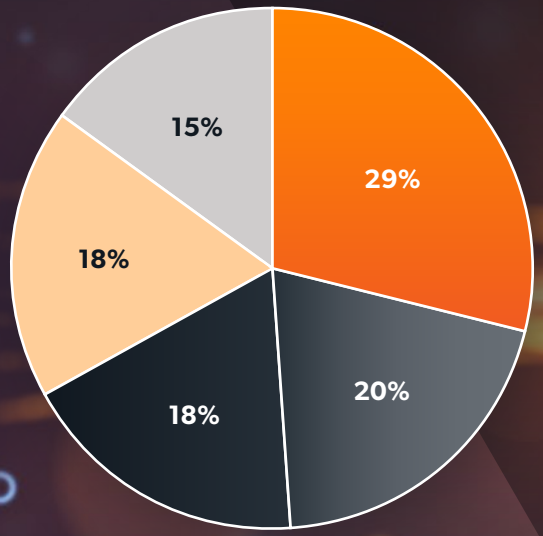
Where participants could choose more than one option, figures are given as a share of all selections recorded rather than a share of participants, with write-in responses included in that denominator. Single-select questions are reported as a share of participants.

Percentages are rounded to whole numbers.

"Channel" refers to the supply side of the industry collectively. Participants selected their own role from four options: Channel Partner, Technology Partner, Consultant, and a write-in Other category. Because these groups face the market rather than operate systems themselves, they are reported together as Channel throughout. End Users, who operate the systems they buy, are reported separately.

Use of artificial intelligence

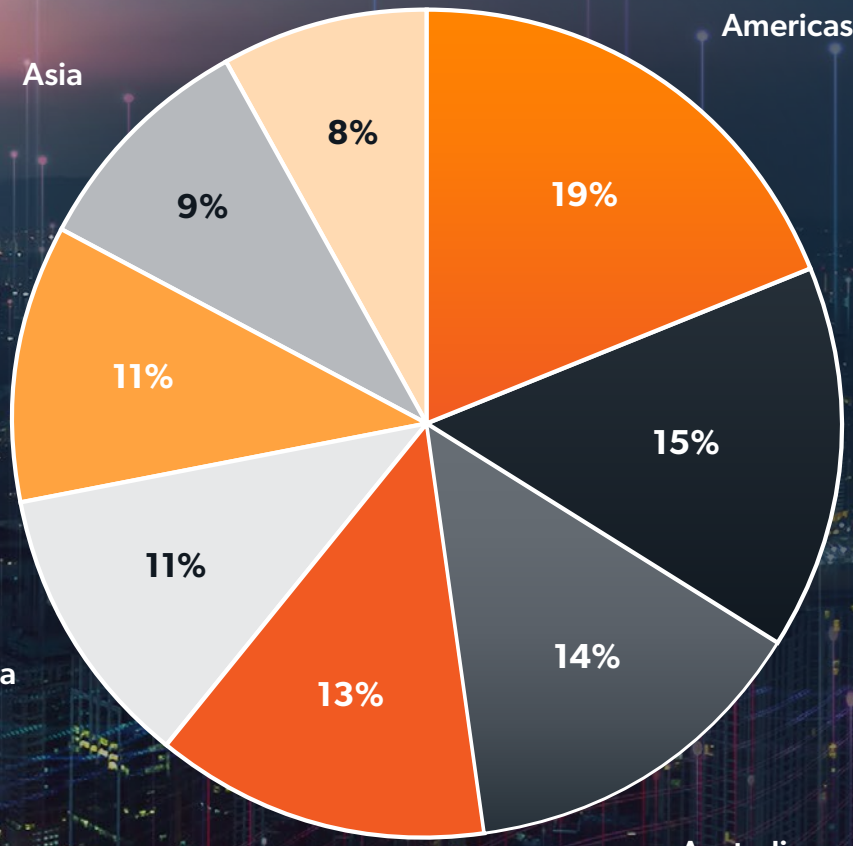
Our team used AI tools to help proofread the report, check calculations, compare figures against our survey data and previous reports, identify external sources, and refine wording. Our team reviewed and verified all AI-assisted content before it was included. The analysis, findings, and views in this report are Gallagher's own, and Gallagher takes full editorial responsibility for the content.



Participant Overview

- End User
- Channel Partner
- Technology Partner
- Consultant
- Other

Participation by Region



Size of Organizations Surveyed



References

Boutin, C. (2024, August 13). *NIST releases first 3 Finalized Post-Quantum Encryption Standards*. NIST. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Data Act explained. (2025, December 15). European Commission. https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

EU Data Act | Recitals 11 to 20. (n.d.). Retrieved September 1, 2026, from https://www.eu-data-act.com/Data_Act_Preamble_11_to_20.html

Framework for financial data access. (n.d.). European Commission. Retrieved September 10, 2026, from https://finance.ec.europa.eu/digital-finance/framework-financial-data-access_en

Hollingworth, D. (2026, June 22). *Accenture closes US$4.2bn OT cyber security deal with Dragos, runZero and NetRise*. Cyber Daily. https://www.cyberdaily.au/security/13781-accenture-closes-us-4-2-billion-ot-cyber-security-deal-with-dragos-runzero-and-netrise

Moschetta, G., Winslow, E., Buys, W., & Hayat, K. (2026). Global Cybersecurity Outlook 2026 Insight Report. *In World Economic Forum*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Payment services. (2025, November 27). European Commission. https://finance.ec.europa.eu/consumer-finance-and-payments/payment-services/payment-services_en

The World Bank. (2021). *Data for Better Lives*. https://digitallibrary.un.org/record/3963929?v=pdf

World Business Council for Sustainable Development. (2026). *Member Insights Report 2026*. https://www.wbcsd.org/resources/most-companies-are-already-assessing-their-physical-risks-but-why-is-implementation-still-a-challenge/?submitted=true

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, productive, and profitable. Security is just the beginning.

Visit security.gallagher.com to learn more

Unlock more



GALLAGHER
Security

