# Security Industry Trends Report 2025

GALLAGHER Security

January 2025
**Author:** Rachel Akbar
**Design:** Jason Lurman

# Contents

# What if We Reimagined Security?

It's my pleasure to welcome you to Gallagher Security's 2025 Trends Report, crafted with input from professionals across the global security industry.

This year's report offers something unique: it goes beyond the data to explore the human elements driving technological shifts and shaping purchasing decisions for businesses around the globe.

It will come as no surprise that security is evolving at a pace we've never seen before. Historically, our industry followed a predictable, cyclical pattern of change happening every 3-5 years. However, with today's rapid technological advancements, those cycles have compressed into mere months.

It's a lot to keep up with, and the End Users we serve are turning to us to make sense of it all.

That's precisely why reports like this matter. They provide a snapshot of this moment in time, contextualizing complex changes so we can all navigate them more effectively.

One of Gallagher's core values is helping each other grow, and our curiosity fuels a commitment to share insights like these with the wider world.

As we compiled this year's findings, we also found ourselves reflecting on the transformations we see - not just in technology, but in how people use, demand, and expect security solutions to serve them. And one question kept surfacing: What if?

What if security was the answer to evolving business challenges? What if it could support shifting workplace norms? What if security was capable of so much more than we've previously imagined?

I invite you to hold that question in mind as you explore this year's report. Let it inspire new ideas and fresh perspectives about where our industry is headed.

**Mark Junge**
**Chief Executive, Gallagher Security**

# Executive Summary

Expanded system functionality and the growing influence of IT are changing organizational priorities and decision-making processes, leading to a greater emphasis on partnership and ease of use.

## Security is becoming a hygiene factor

Businesses are increasingly relying on security systems to deliver broader operational benefits, mitigate staffing shortages, and leverage data for business intelligence. As a result, the process of selecting a system is changing from a focus on features into a much deeper conversation about choosing a long-term security partner.

## Ease of use is top of mind

Expanded functionality is also making ease of use a top consideration when selecting a system. Without a user-friendly interface, complex set-ups risk becoming obsolete as systems gain increased touchpoints with non-technical staff across business units.

## IT is on the rise

As cloud solutions, compliances, and cyber threats become more commonplace, IT departments are gaining a more important seat at the decision-making table and have strong influence over system choice.

## There's a need for education

Misconceptions and a general lack of awareness about system capabilities, emergent technologies, and cybersecurity are major problems among End Users. For Channel Partners, the need for training and upskilling of staff remains a critical necessity.

> ***Delivering an integrated interface for our End Users and simplifying the management of multiple complex systems is one of our key organizational goals for 2025.***
>
> A Channel Partner

## Relationships are underestimated

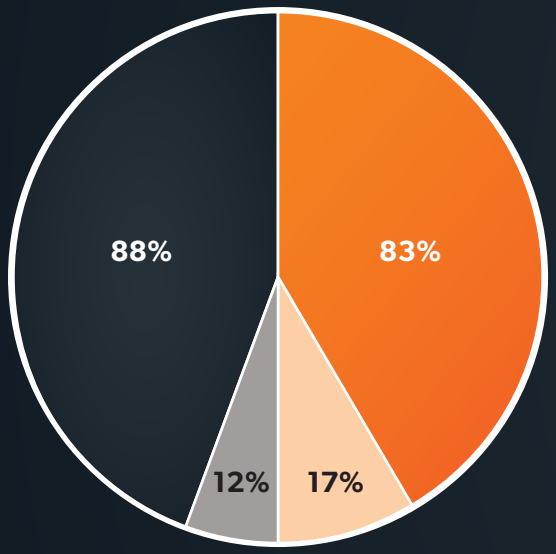
While the industry focuses on advancing technologies, End Users consistently prioritize support, trust, and partnership as their top security needs, suggesting that many security providers are underestimating the importance of building and maintaining strong relationships with their customers.

# 2024 vs. 2025

In 2024, we predicted the industry would lay foundations for growth; in 2025, we'll see End Users and Channel Partners embrace the tools to help them get there.

## What's continuing

- Growth mindset among End Users and Channel Partners
- Security budgets continue to grow or stay the same
- Recognition that upgrades (software and hardware) are critical to business success
- Video reigns king as the top-ranked integration among survey participants




**Security budgets 2024 vs. 2025**

Increase or stay the same 2024

Increase or stay the same 2025

I don't know or decrease 2024

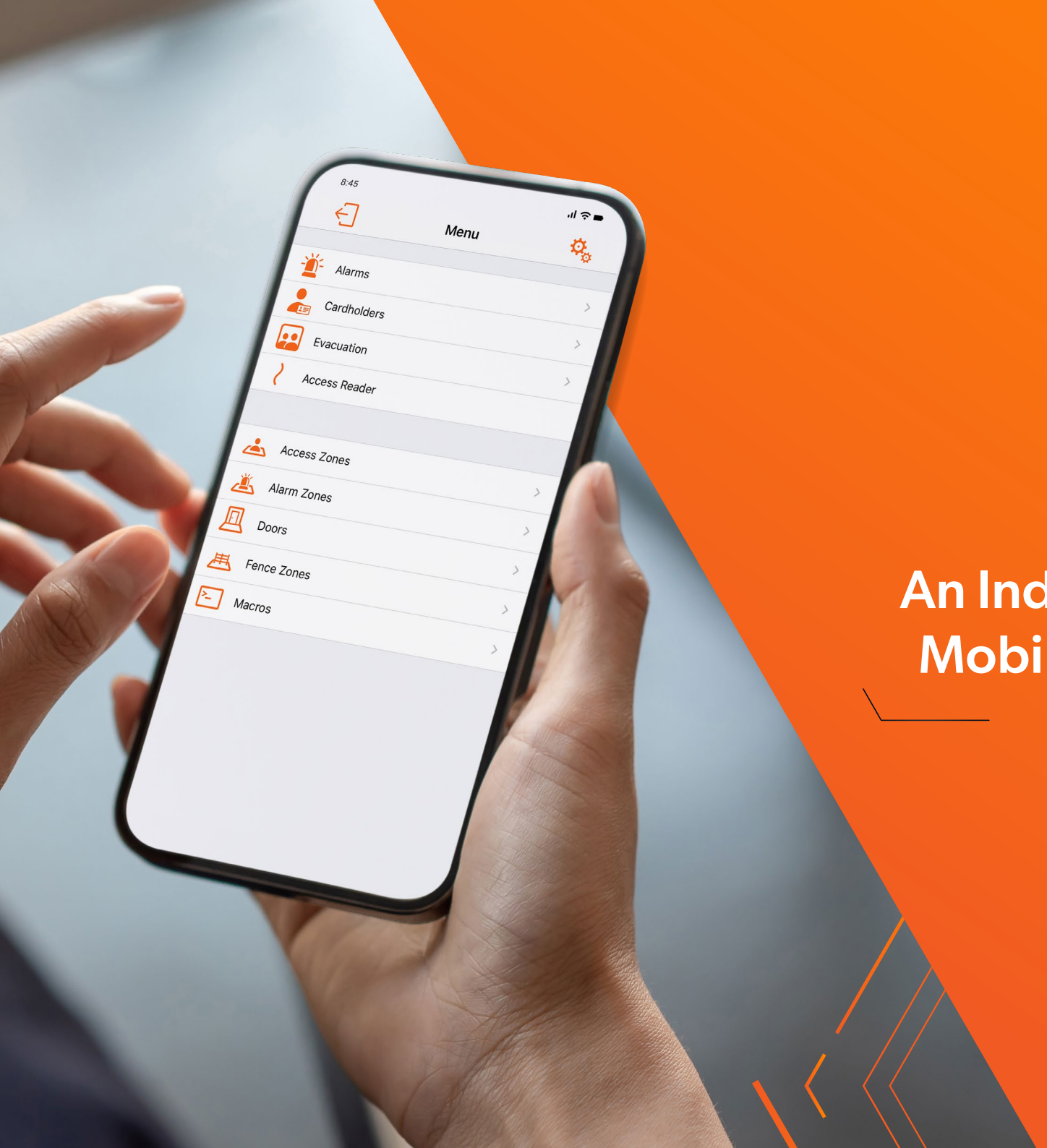
I don't know or decrease 2025

## What's changing

- Increasing comfort with AI
- Demanding more from security systems

> ***[One of our 2025 goals is to] implement advanced threat detection technologies such as AI and machine learning.***

*I would like to prioritize teaching clients analytics and AI for increased user productivity with cameras.*




# An Industry at Odds: Mobile Credentials

**The buzz around mobile credentials reveals growing pains of the industry at large.**

## Key takeaway

In 2024, governments around the world took significant steps toward making digital identification and mobile credentials a global standard.

But a closer look at how this trend is playing out in the security industry reveals a more cautious - and complicated - picture emerging, one symbolic of an industry experiencing growing pains.

# 2024 global snapshot

- The EU Digital Identify Framework launched, requiring member states to offer digital ID to citizens by 2026 (*EU Digital Identity Wallet Home*, n.d.)
- Nearly 70 million Americans across 9 states obtained a digital driver's license, which became TSA compliant in 12 states (Kelleher, 2024)
- Australia announced Trust Exchange, a government-backed digital identity and credentials program (*Trust exchange drives secure digital services*, 2024)
- New Zealand's Digital Identity Services Trust Framework Act of 2023 went into effect (Luczak-Roesch, 2024)
- 37 of the top 50 countries by GDP had implemented digital IDs (Moody, 2024)
- Estonia, India, Nigeria, and Brazil led the world in digital ID adoption (Sever, 2023)

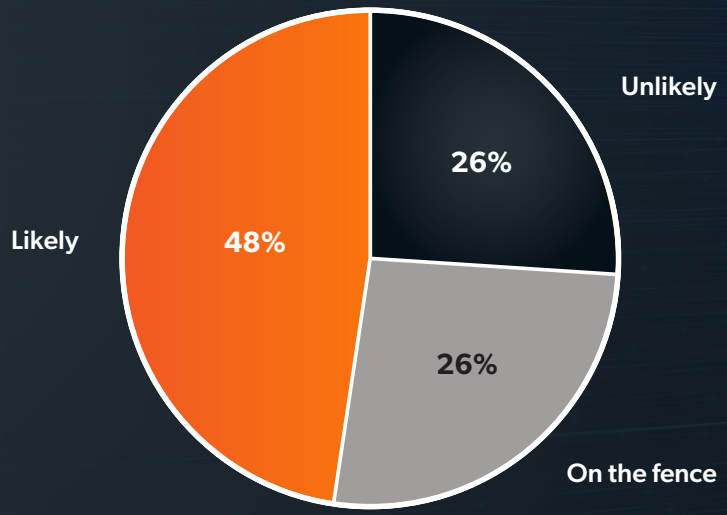
# Security industry deep dive

So why is the security industry moving at a slower pace when it comes to digital, or more specifically, mobile credentials, compared to governments around the world?

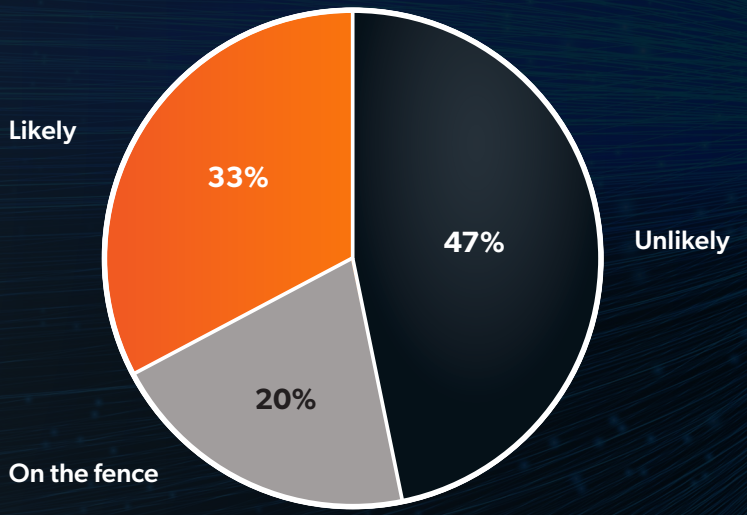
For one, there's a significant split within the industry.

While **48%** of Channel Partners, Consultants, and Technology Partners say their organizations are likely to adopt mobile wallet credentials in the next year, **47%** of End Users say they're *unlikely* to make the change.

## How likely is your organization to adopt mobile wallet credentials within the next 12 months?




Channel Partners, Consultants and Technology Partners




End Users

Notably, the themes of education, IT, and upgrades appear repeatedly in our survey results, revealing some of the core conflicts causing growing pains across the security industry's wider digital transformation.

End Users who say adoption is unlikely cite four common reasons:

### Lack of education

*"Low confidence in end-to-end encryption and understanding it can be done safely"*

*"Lack of information and adversity to change"*

### Policy conflicts

*"Mobile device policies prohibiting personal mobiles for company work"*

*"Policies are written to require badges be worn"*

### IT challenges

*"Challenges with IT department on time, budget, and resources"*

*"Complexities with a shared services IT platform and ensuring it meets all our IT security requirements"*

### Cost of upgrades

*"Cost of hardware replacement"*

*"Current software version does not support and old hardware still in SITU"*

> *Lack of information and adversity to change*

> *Challenges with IT department on time, budget, and resources*

# Cutting Through Misconceptions:

## The Path to Smarter Mobile Credential Adoption

The global surge in mobile credential adoption signals a growing shift towards a premium user experience and a more secure solution for managing access and identity. But while mobile credentials are undeniably a game-changer, they're not a one-size-fits-all solution for all organizations. The truth is mobile credentials aren't for everyone.

Mobile credentials don't support all use cases, and they shouldn't. As our report illustrates, some organizations require a visual identification to be worn by the user, the environment may not be practical for the phone, or organizational policies may dictate phones cannot be used when performing specific duties. There are a number of use cases where mobile credentials simply aren't the right fit.

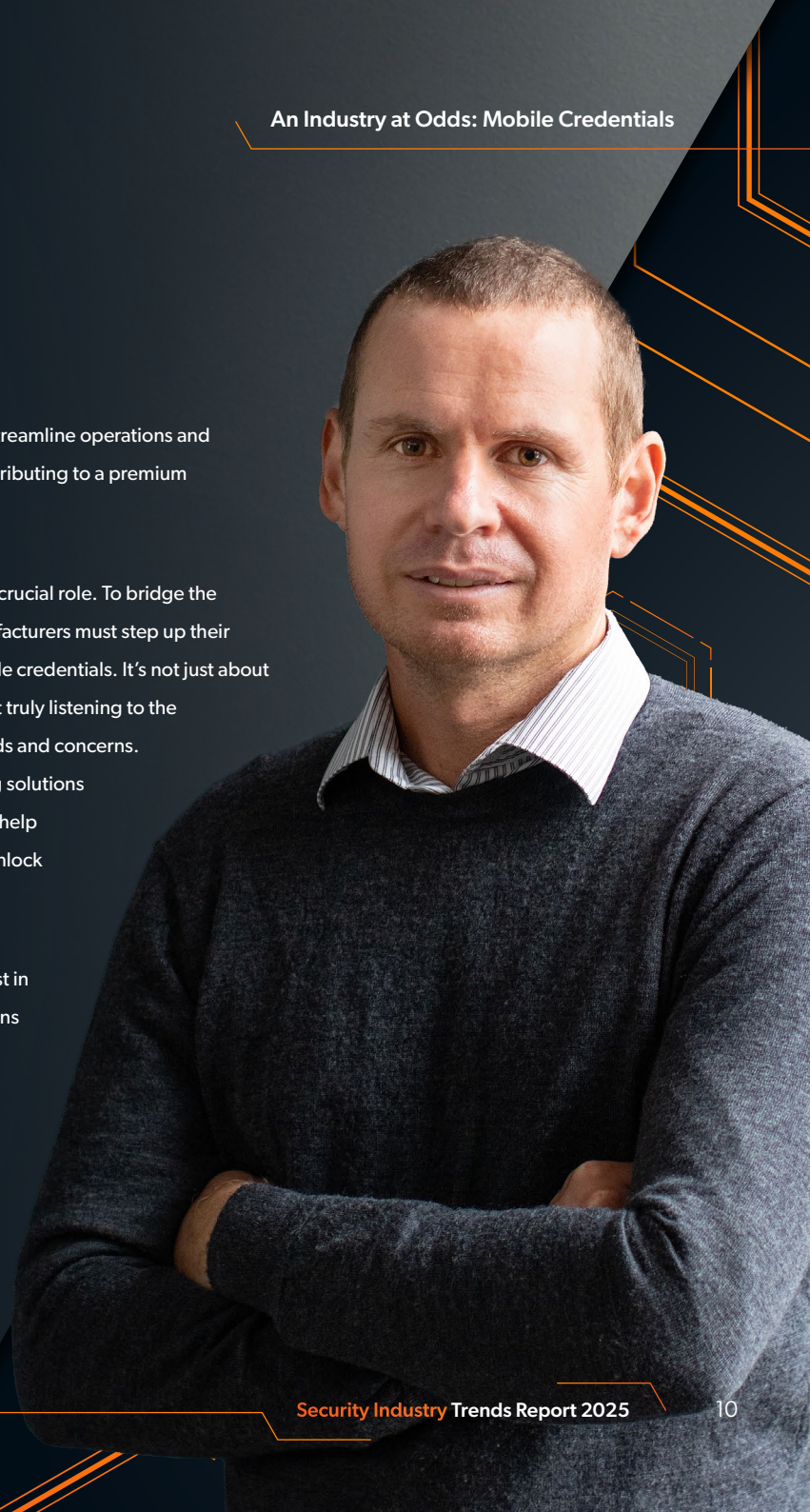
However, this doesn't mean mobile credentials should be dismissed altogether. The key is to recognize that while they might not be universally applicable, they offer significant advantages for many businesses, particularly those looking to enhance flexibility, security, and user experience.

Despite the clear benefits, misconceptions about mobile credentials are widespread, causing hesitation among organizations that would greatly benefit from their adoption. Some believe that mobile credentials are too complex to implement or less secure than traditional methods. These myths often stem from a lack of understanding or outdated information, leading to missed opportunities for businesses to streamline operations and improve security while simultaneously contributing to a premium experience for staff.

This is where security manufacturers play a crucial role. To bridge the gap between perception and reality, manufacturers must step up their efforts in educating the market about mobile credentials. It's not just about touting the technology's features but about truly listening to the customer and addressing their unique needs and concerns. By engaging in open dialogue and tailoring solutions to real-world scenarios, manufacturers can help businesses make informed decisions and unlock the full potential of mobile credentials.

The key to widespread adoption lies not just in the technology itself, but in the conversations we have about it. Let's make sure those conversations are informed, accurate, and, above all, customer-centric.

**Tyson Barnett**
**Product Manager - Credentials**



# People

**People are impacting the finer points of the industry's digital transformation – but often, it's overlooked.**

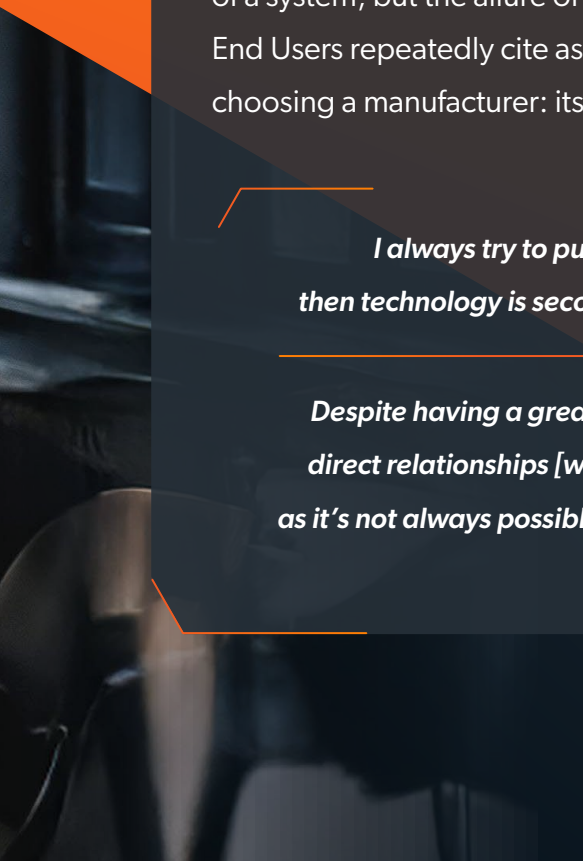
## Key takeaway

Cutting-edge technologies have long been touted as key selling points of a system, but the allure of advanced features often overshadows what End Users repeatedly cite as the most important consideration when choosing a manufacturer: its people.

> *I always try to put [the manufacturer's] people first, then technology is second, then standards, and the last is price.*

> *Despite having a great relationship with our Channel Partner, direct relationships [with the manufacturer] are still important as it's not always possible for partners to communicate on change.*

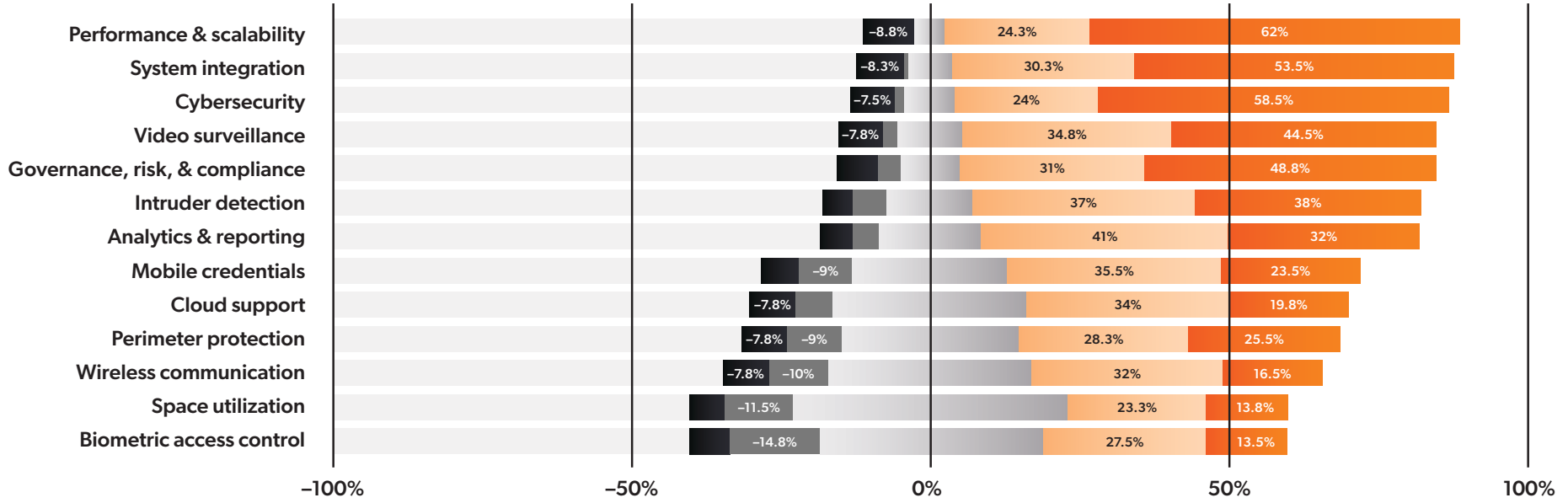
> ***First and foremost, the top consideration should be the people (staff) that work for the company. Companies don't do business, people do business!***



# People-first system prioritization

Performance, scalability, cybersecurity, and integrations remain the top-ranking system capabilities identified by survey participants. Broken down further, video continues to reign supreme as the most important integration identified by organizations.

**Rank the security system features and technology in order of importance to you and your organization and/or the organizations you work with.**



However, when asked to identify the most important factor organizations consider when choosing a security system, a more people-focused image emerges emphasizing support, reliability, and ease of use.

## Support

*"End user support & training"*

*"Support from tech support and dealer rep"*

*"Support & maintenance"*

## Reliability

*"Reliability and after-sales support"*

*"Reliability and manufacturer support"*

*"Reliability, usability and technical support of the platform"*

## Ease of use

*"Ease of implementation and user friendly for the End User"*

*"Easy to work with, intuitive"*

*"Ease of use at an administration or operational level"*

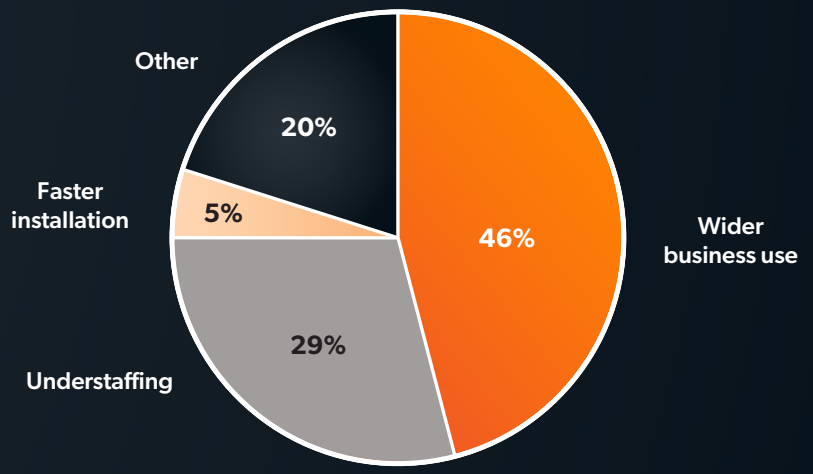
> *Ease of implementation and user friendly for the End User.*

## Key drivers behind ease of use

A LinkedIn survey indicates that wider system use throughout businesses is the key driver behind these prioritizations, with one participating Consultant saying, "ease of use [and] ease to administer has trumped truly secure access control solutions for decades" (Anonymous, 2024).

**46%** of participants state wider business use as the key cause with **29%** pointing to ongoing staffing struggles.

### Why ease of use matters



# Staffing and training

Staffing remains a top challenge faced by organizations, particularly for Channel Partners who say the issue is snowballing into larger business problems, including:

## High staff turnover

*"FTE count is abysmal for the size of the system we are dealing with."*

*"High staff turnover rates are impacting our operational efficiency and continuity. Constantly hiring and training new employees takes time and resources, disrupting workflow and productivity."*

## Rising costs

*"Capable staff are in short supply and are enjoying generous salaries at present in a market where margins are being squeezed."*

*"Rising costs across various aspects of our operations, including materials, labor, and technology, are putting pressure on our budget and affecting our profitability."*

## On-the-job errors

*"Inexperience is hurting our business, from ordering wrong parts to not having a proper understanding of products."*

*"Installations done incorrectly by untrained service providers are costing us time and money."*

## Growth restrictions

*"We need to employ more technicians as our client database is expanding."*

*"The shortage of experienced personnel affects our ability to innovate and maintain our systems effectively."*

*The shortage of experienced personnel affects our ability to innovate and maintain our systems effectively.*

## Top challenges faced by Channel Partners

For many, the solution is training. However, the realities of training present their own challenges:

> ***"Keeping on top of staff training and certifications is a challenge. With a high turnover of techs in the industry currently, getting new techs trained is becoming very cost and time prohibitive."***

As a result, many Channel Partners are turning to manufacturers to help plug the gaps: ***"Obtaining reliable and honest support from our suppliers and manufacturers could help us work around some of these [staffing] problems."***

# Partnership is redefining access

As staffing and training challenges see no end in sight, new expectations on partnership are emerging within the security industry. Overwhelmingly, survey participants told us that partnership means access, but not in the way the industry has traditionally defined it.

Partnership means access to…

*"…technical and sales personnel willing to think outside the box"*

*"…online support and technical BDMs that know the product well"*

*"…information and product experts"*

*"…technical experts with clear communication"*

*"…good support"*

*"…training"*

*"… information without having to book a call"*

**In short, technology is only half of the equation in today's security environment - access to people and their expertise is the other.**

# From Legacy to Innovation:
## Attracting the Next Generation of Security Professionals

My career didn't start in security, it began in dental.

My time there was brief, largely because when an opportunity to join the authentication field arose, I immediately jumped at the chance and haven't looked back. There was an excitement about joining a tech-forward industry that hasn't waned for me, even though it's been over a decade since I made that leap.

When I reflect on where I was at that time in my life - still fresh out of college and eager to be a part of something bigger than myself - I wonder why our industry isn't doing more to attract equally fresh and eager candidates to our field.

The security world has been led by professionals with decades of experience under their belts, and while this knowledge is undeniably invaluable, our growth is dependent on new perspectives, particularly from those well-versed in today's advancing technologies.

Younger professionals have the massive advantage of being digital natives, accustomed to integrating technology into their daily lives. They're more comfortable with software-driven solutions, cloud computing, AI, and data analytics, all of which will soon become foundational elements of forward-thinking security operations. This group brings an electric energy and inclination to challenge the status quo, questioning outdated practices and pushing for contemporary alternatives.

They might ask why access control systems aren't yet integrated with AI-driven video analytics, or why cloud solutions aren't more widely adopted for security management. Their instinct is to drive innovation, embracing new technologies that align with the industry's ongoing digital transformation.

Organizations that embrace this new wave of talent are already seeing the benefits. For example, younger professionals are helping bridge the gap between physical security and IT, which has often been seen as more progressive in its adoption of advanced technology.

The seasoned professionals of our industry have ensured that the values driving security forward are well embedded in our foundation. Now, it's time for the rest of us to honor those efforts by ensuring the work they've started is carried out by future generations.

**Natalie Bannon**
**Director of Strategic Alliances**

# Shifting Foundations

**As we approach the other side of the digital transformation, what will the foundational elements look like?**

## Key takeaway

A clearer picture is emerging in 2025 that shows businesses fortifying their investments in **cybersecurity, cloud solutions, and AI** as part of their digital transformation - but it's not without reservation.

# Cybersecurity

As organizations embrace cloud solutions and AI tools, they're also increasing initiatives to strengthen cybersecurity measures and build a stronger culture of risk awareness.

The challenge lies in balancing the benefits of these evolving technologies with a hesitancy borne from lack of awareness and education among staff, a major pain point standing in the way of organizations achieving their cybersecurity goals.

## Goals and challenges for 2025

*"Overcoming the lack of understanding on the importance of upgrades to ensure cyber compliance"*

*"Education in unforeseen risk; cybersecurity and OT network vulnerability"*

*"Correcting human mistakes like clicking on links"*

*"Adaptation to emerging threats and data protection while maintaining cost efficiency, scalability, etc."*

*"Aligning with internationally recognised standards whilst maintaining the business objectives"*

# The cloud

In 2024, we reported that Channel Partners were embracing the shift to cloud-based solutions faster than End Users. Moving into 2025, it appears the gap is closing - with some notable exceptions.

Across the board, survey participants cite greater access and control, ease of use, and cost savings as key benefits driving cloud migration.

## Cloud migration drivers

### Greater access and control

*"Ability to control and manage a system from anywhere"*

*"Ability to manage data off site, potential for other parties to manage as a service"*

### Ease of use

*"Ease of network configuration, ease of increasing system performance and capacity at the click of a mouse, ongoing support"*

*"Easy to manage, up-to-date software, use anywhere"*

### Cost savings

*"Choice, reduction of space and cost, flexibility"*

*"Cost savings and offsite data storage and protection"*

# Cloud migration barriers

However, the cost of migration is also a barrier to adoption along with concerns about infrastructure and cybersecurity.

## Cost

*"Additional costs"*

*"Ongoing costs"*

*"Potentially higher ongoing cost"*

## Infrastructure

*"Adopting cloud solutions remains a challenge because of infrastructural deficit"*

*"It's a nightmare trying to move all systems to the cloud"*

*"Migrating to the cloud means additional work when deploying or maintaining a system as the system server is not accessible"*

## Cybersecurity

*"Cybersecurity risks associated with third party providers that need to be covered"*

*"If we were to deploy more cloud-based features, we would need a strong assurance that the security of the system is as strong as it can be, and vulnerabilities are identified and patched as soon as possible"*

*"Not safe for us due to the fact that we don't know who hosts the servers and administrators of them"*

Cloud migration is also part of a larger ongoing compliance conversation with IT departments.

Some believe the move will simplify system management and introduce stronger cybersecurity measures that reduce IT's involvement. However, others see the cloud as increasing dependence, causing conflict between departments.

## Reduced IT

*"Having a secured system without having to depend on clients getting involved and working with IT"*

*"Cloud becomes easier to manage for organisations managed by IT departments to allow for easier updates and management"*

*"Ease of network configuration"*

## Increased IT

*"Complexities with a shared services IT environment"*

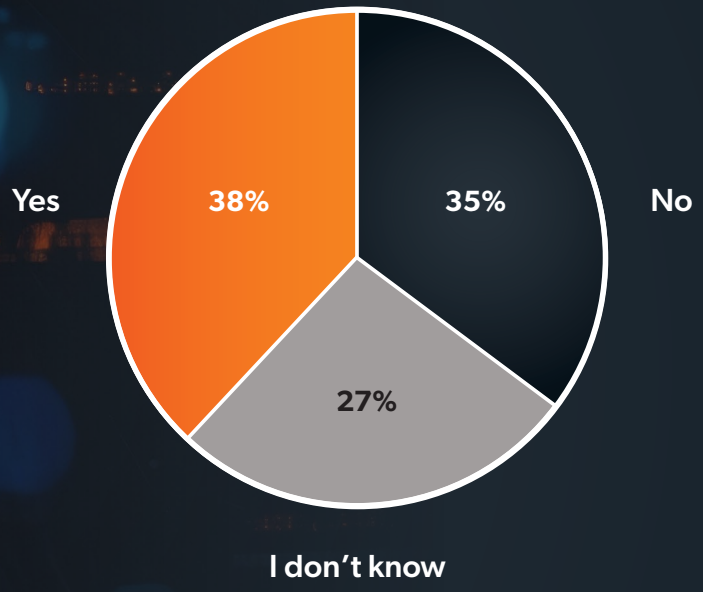
*"Cloud requires increased IT expertise within business, but we have no dedicated IT department"*

*"We are open to cloud-based solutions; however, our IT department is very involved with the deployment to ensure all policies are still met and we ensure that our interactions with the product are protected"*

# AI

Organizations remain split on the implementation of AI tools, but as technology improves alongside persistent business problems, many are looking ahead at how they may be incorporated in the near future.

## Has your organization implemented AI tools or integrations?




Those who **object** to the use of AI tools cite **privacy**, **performance**, and **training** as their chief concerns.

### Privacy

*"'Big brother' fears and a lack of clear policies and procedures"*

*"Concern on security - data / IP"*

*"GDPR and Data Protection Laws"*

*"I don't believe we should trust AI at all"*

### Performance

*"AI isn't doing enough to warrant the cost yet"*

*"AI vendors over-promising and under-delivering, high resource requirements, shortage of AI experts in our teams"*

*"Bad results"*

*"Early stages of tech"*

### Training

*"Confidence to use"*

*"Cost and lack of understanding"*

*"Education and maturity of technology"*

*"Investing in the right talent, ensuring high-quality data, managing change effectively, and developing ethical guidelines and security measures to govern AI use"*

However, those who are eager to adopt AI tools do so because ***"AI puts hours back in a day,"*** it ***"assists with admin work,"*** and it ***"has cost savings to the End User due to using fewer systems to monitor a site."***

Increased adoption of AI tools was also a common response to the question "What are the key goals for your security system over the next 3 - 5 years," indicating the tide may be close to turning on AI acceptance.

# What does hybrid really mean? Hint: It doesn't matter

The term "hybrid cloud" gets tossed around a lot in the security industry, often with an air of certainty. But ask ten people to define it and you'll likely get ten different answers. Is it about balancing on-premise systems with cloud platforms? Is it a strategy for seamless multi-cloud integration? Or is it something else entirely?

**Here's the truth: it probably doesn't matter.**

Hybrid cloud deployment means different things to different organizations because no two businesses have the same starting point, priorities, or challenges. For some, hybrid might be the perfect bridge between customer infrastructure and scalability. For others, it's a tactical choice, dictated by compliance or data residency requirements. And for many, it's a constantly evolving mix of solutions that defies neat categorization.

The real question we should be asking isn't "what does hybrid really mean?" but "why does this matter to my organization?" The industry's obsession with rigid definitions risks overshadowing what truly counts: outcomes. Are you achieving greater flexibility? Improving security posture? Delivering value to your stakeholders?

As time marches on and hybrid cloud solutions become the norm rather than the exception, we must embrace its fluidity. The future of enterprise solutions doesn't hinge on consensus over terminology, but on a shared commitment to adaptability and innovation.

After all, the beauty of hybrid cloud deployment is that it isn't one-size-fits-all. And that's what makes the concept so powerful.

**Guy Irvine**
**Value Stream Lead - Future of Enterprise / SMB**

# Expanding Value

**By reimagining the potential of security systems, businesses are unlocking new value and transforming how they operate.**

## Key takeaway

Organizations are leveraging security technologies in innovative ways to address diverse challenges, unveiling new functionalities that extend the capabilities of traditional security in the process.

As a result, End Users are raising the bar for the industry at large and creating new expectations for what systems can - and should - deliver.

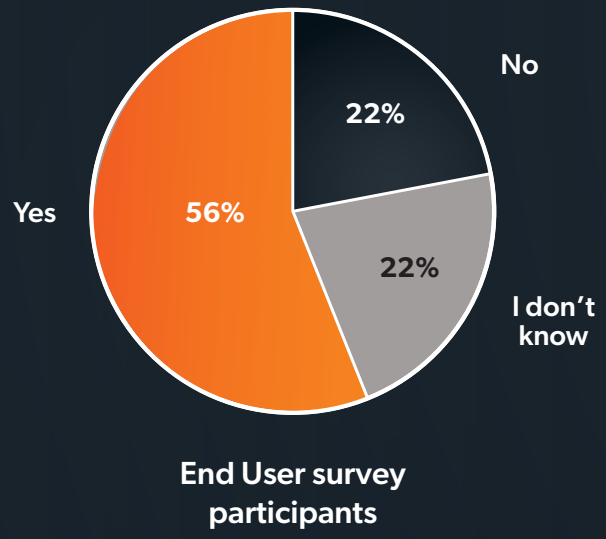
# Operational efficiencies

Operational inefficiencies can cost businesses upwards of 20 - 30% of revenue each year, causing many to try and solve the problem by hiring third-party consultants or introducing new systems that promise to staunch the bleeding (Duncan, 2023).

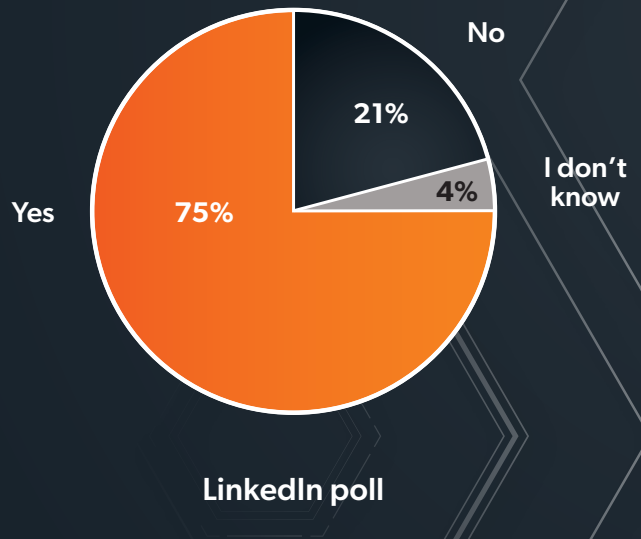
But as more businesses realize their existing security system contains creative operational solutions, the tide is turning on how efficiency is managed.

## Strategies in place for operational efficiency

**56% of End Users** surveyed and **75% of participants** in a LinkedIn poll currently have strategies in place for using their security system to increase general operational efficiency.




End User survey participants




LinkedIn poll

Examples of efficiencies organizations are gaining from their system include:

*"Cafeteria meals planning using building occupancy, cafeteria utilization, man hours reports, customer visits reports"*

*"Time and attendance reporting, alcohol and drug testing, fatigue management"*

*"Linking with HR systems"*

*"Confirming if equipment is running and producing a quality product"*

*"To protect workers through location tracking, remote operations, and monitoring of hazardous work areas"*

*"Reduce operational costs with real-time visibility of assets that identifies potential issues early, helping extend asset life"*

*"Lighting and HVAC control"*

*"Use of mobile credentials for casual staff to avoid loss of access fobs. Introduction of access control to controlled drugs safes"*

*"We currently make use of vehicle monitoring and tracking and digital workflow management"*

*"We utilize the security system to call meetings, register visitors, and action our regulatory requirements (fire drills, etc.)"*

*"Access credentials used for other purposes, eg vending machines or ICT equipment"*

*Overwhelmingly, the number one operational efficiency survey participants are deploying is system automation. It's largely being done to solve staffing problems and alleviate workloads, but as businesses count the tangible benefits automation delivers, it may also be paving the way for increased acceptance of AI tools.*

*"Automate and transform to a digital/less physical access control world"*

*"Automation of reporting and increased protection and staff management"*

*"Automation of manual tasks"*

*"Automation of onboarding and profile changes to access assignment and termination based on data from our people and student systems"*

*"Automation of processes"*

*"Automated threat detection and response"*

# Data and intelligence

Organizations are also using systems beyond their traditional roles to extract actionable intelligence and make smarter, data-informed decisions, such as:

*"Collecting data to provide insight on facilities usage"*

*"Data analytics and reporting for enhanced communication, energy and resource management, and training and simulation"*

*"We use our corporate real estate data to identify access trends"*

*"Provide business intelligence data to streamline repetitive tasks"*

*"Boost productivity by sharing information across all processes and business applications"*

*"Developing our business plans and strategies"*

*"High level corporate strategies"*

*"Increasing safety through site reporting"*

*"We have recently conducted a substantial amount of work to create clear delineation between the different agencies which have access to our tenancies by bolstering our reporting capabilities"*

***Collecting data to provide insight on facilities usage***

# Sustainability

Sustainable practices have been gaining traction thanks to increased education, global legislation, and more options to help organizations enact change. **60%** of participants affirmed their organization has sustainability strategies in place.

*"Footprint shrinkage"*

*"Green infrastructure and life cycle management"*

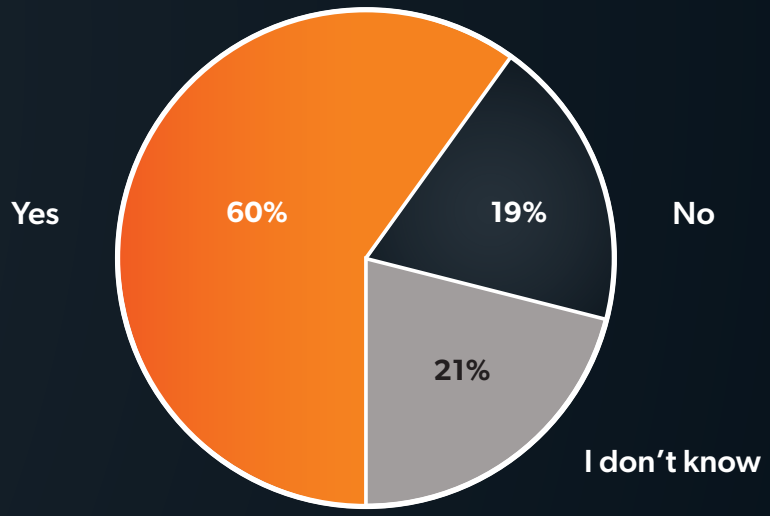
*"Minimizing waste generation and promoting recycling. Engaging with local communities on sustainability initiatives"*

*"Power production and waste management"*

*"Recycling, power savings, carbon offsets"*

*"We have a Kaitiakitanga Environmental Sustainability strategy, and one of our five aims is 'Building Sustainability for Future Generations.' We have just achieved Toitū carbonreduce certification for a second year."*

**Does your organization currently have strategies in place around sustainability?**



# Beyond Buzzwords:
## The Power of Purpose-Driven Innovation

Twenty-five years ago, I lost a battle that haunts me to this day: I agreed to sell my 1973 Mazda RX3 Rotary in exchange for a 1997 Ford Mondeo Wagon.

In a contest, the RX3 Rotary wins out on pride, but my wife insisted that the Mondeo Wagon would fit our new baby's pram better, and that beat out the Mazda's cool factor by a mile. I would have loved to keep that car, but it didn't serve my family, which meant it wasn't the right vehicle to drive us forward.

I've been thinking about that decision a lot lately because I've been hearing the buzzword "innovation" pop up over and over. As an industry, we talk about our individual products as being innovative - and I understand the impulse to do so. Even in the last ten years, our industry has made leaps and bounds that seemed unimaginable at the time, and it's worth celebrating those developments.

But when we talk about innovation, products are just one part of a much bigger story.

Innovation isn't about individual components: it's about the vision of what goals can be achieved, barriers can be broken, and new benefits can be gained by combining those components to create innovative solutions.

It's why I've been thinking back to my RX3 lately. I doubt anyone would call the 1997 Ford Mondeo Wagon a particularly innovative vehicle, but it was a solution that empowered my family to go places we couldn't have gone otherwise. In other words, it was transformative for us, and I'd call that innovative.

Don't get me wrong - I still think our industry should be enthusiastic about developing leading-edge technologies. But we should remember that innovation also means empowering people to be more connected with each other, their behaviors, and their goals - and most importantly, to protect those connections once they're made. That's true innovation, and that's where Gallagher Security is headed.

**Merv Williams**
**Chief Marketing Officer**

# Word on the Ground: Regional Insights

## Brad Small, Regional Sales Manager - New Zealand

*"There's a serious need for simplified system installation. It's not just about decreasing the cost that an End User pays for a system - it's also about making installations faster so that more can have their security needs met without having to wait. Waiting means vulnerable people and assets."*

## Jack Meltzer, Consultant Program Manager - Americas

*"I see a rising trend of consulting firms providing managed services to End Users that have traditionally been provided by Channel Partners. It's changing the dynamics of the market and I'm curious to see how Channel will adapt to the changes."*

## Travis Lee, Business Development Manager - Asia

*"I've seen a growing shift from traditional access cards to alternative credentials such as QR codes, facial recognition, and mobile credentials. These technologies are gaining traction due to their enhanced convenience, improved security, and alignment with the region's digital transformation efforts in both commercial and residential sectors."*

## Khodor Habbouche, Sales Director - Middle East

*"There's a growing trend towards the integration of smart building technologies driven by the need for enhanced security and energy efficiency. As businesses and governments increasingly prioritize sustainability, smart solutions are becoming essential in the construction and management of buildings."*

## Pedro De Jesus, Sales Manager - Queensland (Australia) & Papua New Guinea

*"The demand for technical skillsets is greater than supply, impacting all sectors within the security ecosystem. As a result, customers are investigating options such as SaaS, managed services, AI, and augmented reality to do more with less and introduce competitive advantage. Understanding the best combination of pathways is extremely challenging and I am keen to see this play out in market over the coming years - those who introduce organizational readiness and adapt will lead."*

## Bethan Thompson, Regional Marketing Manager - United Kingdom & Europe

*"There's a palpable excitement at events that has finally returned in the post-pandemic years. People are more engaged, loving being face to face, and the conversations happening on trade show floors are of a much higher quality than in previous years. I don't think it's a coincidence that trade show growth is happening alongside innovative development within our industry."*

## Nico Smit, Technical Business Development Manager - South Africa

*"Estate security is a major trend across Africa. Measures like biometric impassable credentials, visitor management, and integrations with perimeter are core elements for securing families and communities. They also contribute to the larger goal of building safer cities, where technology plays a pivotal role in crime prevention and emergency response."*

# Relationships:
## The Foundation of Innovation

I'm proud to see how Gallagher's core values - respecting all voices and harnessing the power of diverse experiences - shine throughout this year's report. When we embrace every perspective, we uncover the insights needed to drive exceptional outcomes for all, from the End Users challenging us to innovate to the Channel Partners and Consultants whose expertise has been honed over decades.

Among the diversity of perspectives present in this year's report, one truth rings loud and clear: technologies will evolve, but the cornerstone of success will always be the value of relationships. Whether it's with long-time partners or new voices shaping the future, the relationships we build are the foundation of everything we do.

As we look to the year ahead, let's prioritize these connections. Attend industry events, meet your customers face-to-face, truly listen to their needs, and foster the trust this year's report tells us people are craving. By investing in people as much as we invest in technology, we'll not only meet the demands of tomorrow, but also strengthen the bonds that make our industry resilient and thriving.

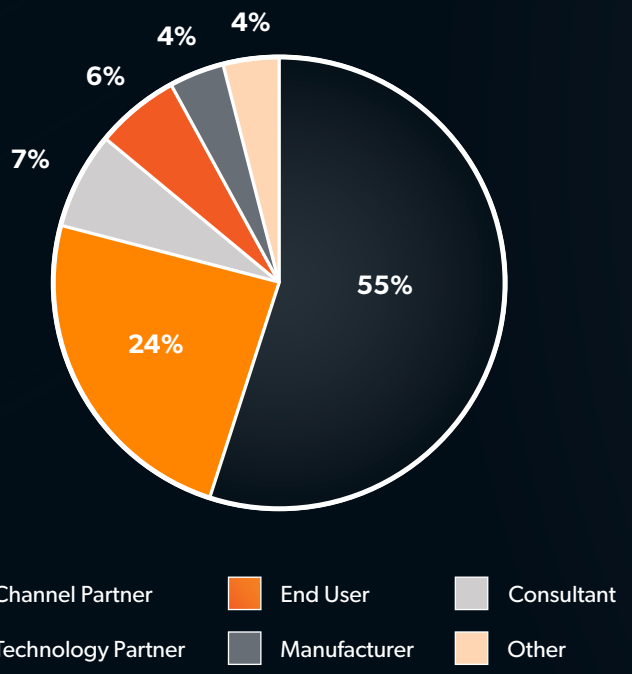
Together, let's keep building, innovating, and growing - one relationship at a time.

**Meredith Palmer**
**Chief Product Officer**

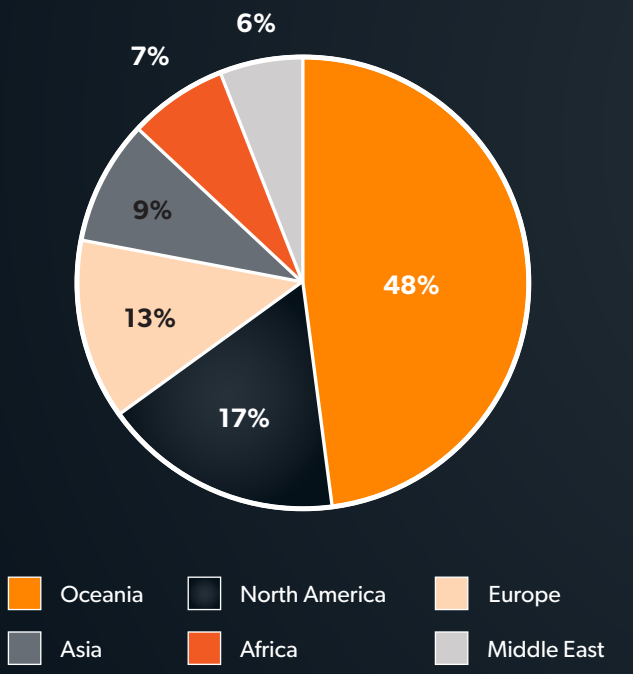
# Methodology and Demographics

From June 3 to July 31, 2024, Gallagher Security surveyed global security professionals and End Users with the intent of understanding the future of their organizations and what they perceive as the most important issues relevant to their security systems in the year(s) ahead. Surveys were distributed across Oceania, North America, Europe, Asia, and Africa.

## Participant overview




## Respondents by region



# Participants' roles

## End Users

- Manager (Security, Facilities, Site, IT, Project)
- Lead (Critical Infrastructure, Digital Systems, Safety & Security)
- Security Advisor
- Director (Security, Risk, Network, Engineering)
- Head of (Building Technology, Security & Logistics)
- Chief Operations Officer

## Channel Partners

- Technician
- Engineer
- Manager (Business Development, General, Account, Regional, Sales, Communications, Technician, Service, Sales, Department)
- Director (Managing, Project, Operations, Sales, Technical, Marketing)
- VP Sales
- Chief Technology Officer
- Chief Executive Officer

## Consultants

- Consultant (Security, Managing, Physical Security, Principle, Technology)
- Manager (Integration, Project)
- Director (Risk, Managing)

## Technology Partners

- Engineer
- Manager (Account, Category, Regional, General, Sales, Technical)
- Director (Sales, Regional, Managing)
- Chief Executive Officer

## Manufacturer

- Manager (Sales, Business Development, Regional, High Security, Channel, Technical)
- Vice President (Regional, Product, Engineering)
- President (Regional)
- Chief Executive Officer

# References


Anonymous. (2024, August 10). *What is behind the uptick in users calling for ease of use?*. [Post]. LinkedIn. https://www.linkedin.com/posts/gallagher-security_increasingly-organizations-report-that-ease-activity-7226709454229028866-jNzg?utm_source=share&utm_medium=member_desktop

Duncan, R,D. (2023, March 28). *Drowning in unnecessary work? Here's your life preserver.* Forbes. https://www.forbes.com/sites/rodgerdeanduncan/2023/03/28/drowning-in-unnecessary-work-heres-your-life-preserver/

*EU Digital Identity Wallet Home*. (n.d.). European Commission. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

Kelleher, S. R. (2024, June 12). *TSA now accepts digital IDs from these nine states.* Forbes. https://www.forbes.com/sites/suzannerowankelleher/2024/06/12/tsa-digital-ids-nine-states/

Luczak-Roesch, M. (2024, July 9). *NZ is moving closer to digital IDs – it's time to rethink how we protect our valuable data:* Markus Luczak-Roesch. NZ Herald. https://www.nzherald.co.nz/nz/nz-is-moving-closer-to-digital-ids-its-time-to-rethink-how-we-protect-our-valuable-data-markus-luczak-roesch/LQE5Q5VZBFFIRBXNTFQRKNPC2M/

Moody, R. (2024, February 1). *Digital IDs: 50 countries ranked by digital ID requirements and use*. Comparitech. https://www.comparitech.com/blog/vpn-privacy/digital-ids-study/

Sever, A. (2023, April 12). *Digital identity in developing countries: What lessons can be learned?* Forbes. https://www.forbes.com/councils/forbestechcouncil/2023/04/12/digital-identity-in-developing-countries-what-lessons-can-be-learned/

*Trust exchange drives secure digital services*. (2024, August 13). https://ministers.dss.gov.au/media-releases/15621

# 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, defence, commercial, industrial, healthcare, transportation, mining, and educational organizations in 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**


GALLAGHER
Security

GALLAGHER
Security

security.gallagher.com