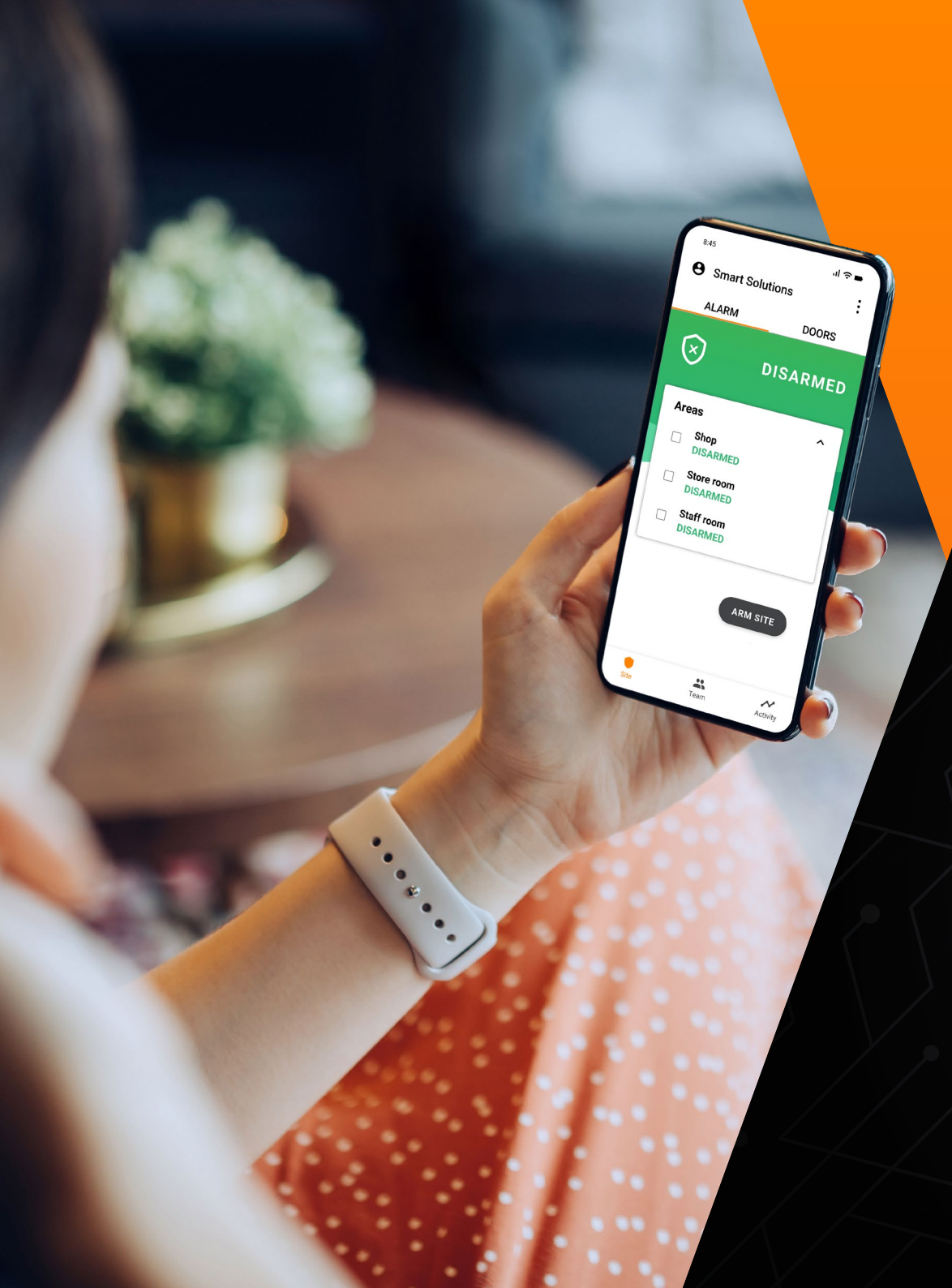


Security Industry Trends Report 2024

Key insights shaping the security landscape from
End Users, Channel Partners, Consultants, and industry experts

GALLAGHER Security

Contents

Charting New Horizons: Research and Customer Connection **3**
Executive Summary **4**
Current and Future State of Organizations **5**
Key Takeaways 6
Safeguarding the Digital Frontier: The Imperative of Upgrading Security Software and Hardware 9
Prioritization of Security Capabilities 10
Operational Changes Due to Pandemic 12
The Cloud 13
Organizational Challenges **14**
Key Takeaways 15
The Power of Training: Bolstering Employee Retention and Tackling Skills Shortages 16
Top Challenges Faced by Organizations 17
Security System Prioritization **18**
Key Takeaways 19
A Transformative Path Forward: Embracing the Potential of Cloud-Based Security 20
System Integrations 21
Security Features and Technologies Most Important to Organizations 22
Manufacturer and Supply Chain Visibility 23
Importance of Cybersecurity **24**
Key Takeaways 25
Setting a Higher Standard: Fortifying Cybersecurity to Face the Unknown 26
Implementing New Cybersecurity Capabilities 27
Unlocking the Potential of Data and Analysis **29**
Key Takeaways 30
Making Data-Driven Decisions Through Access Control 31
Intelligence Through Data 32
The Adoption of AI 33
The Importance of Listening: The Customer as Compass **34**
References **35**
Methodology and Demographics **36**
About Gallagher Security **40**

December 2023
Authors: Rachel Akbar & Pascale Howell
Design: Jason Lurman

GALLAGHER Security

Charting New Horizons:

Research and Customer Connection

It's with great enthusiasm that I present the inaugural Gallagher Security Industry Trends Report for 2024. This report marks a significant milestone in Gallagher's enduring commitment to research and development and we're excited to share what we've learned about the direction of the industry with the wider security community.

This past year the security industry has seen a continuity of challenges stemming from the Covid-19 pandemic and ongoing international conflicts: supply chain issues continue to disrupt business as usual, impacts of labor market shifts continue to linger, and global financial uncertainty coupled with the regularity and impacts of cyberattacks continue to grow. .

Throughout July and August 2023, we surveyed a global mix of End Users, Channel Partners, Consultants, and Technology Partners to learn directly from them about the challenges they're facing, how their organizations are prioritizing security efforts and budgets, and what they're planning for the year ahead.

Our decision to produce this report was rooted in one of our core values: the belief that sharing knowledge freely can serve as a powerful catalyst for growth and progress. This document serves as an embodiment of those values and the customer-centric focus that guides our decision making. Whether it's safeguarding a country's electrical grid or protecting a small business owner's first venture, people are at the heart of everything we do at Gallagher, and this report reflects that focus.

We hope the insights contained within these pages will facilitate meaningful dialogue, inform strategic decisions, and foster a more secure and connected industry for all.

Mark Junge
Chief Executive, Gallagher Security

GALLAGHER Security

Executive Summary

Organizations are at a technological crossroads heading into 2024: there's an eye on growth, but several roadblocks pose challenges to achieving that goal.

Security budgets are predicted to increase in the new year, but with the looming threat of a recession and inflation continuing to rock local economies, those budgets may be allocated to fortifying existing systems before End Users are prepared to explore new technologies (Conerly, 2023). For Channel Partners and Consultants, promoting upgrades and installing video surveillance will likely be major opportunities.

Staffing and training

End Users, Channel Partners, and Consultants all identify recruitment and retention as major pain points, citing a lack of skilled technical staff as a particular challenge. Moving into 2024, all three plan to prioritize hiring and the upskilling of existing staff.

Video integrations

Surveillance is the top integration priority for End Users who repeatedly identify video as the most-needed addition to their current system, with plans to invest in these solutions now and into the new year.

> **A transition from basic defenses to innovative solutions is on the horizon**

Cybersecurity

End Users, Channel Partners, and Consultants all recognize the need to strengthen their cybersecurity efforts with an emphasis on upgrades to existing systems and the education of staff. A transition from basic defenses to innovative solutions is on the horizon, but building a strong foundation is the priority for 2024.

Cloud solutions

There's an increasing recognition by Channel Partners that transitioning to cloud-based solutions is inevitable, but End Users are slower to prioritize their adoption. Those who do plan to deploy cloud solutions anticipate incorporating them as part of a hybrid deployment strategy with their organizational systems, with a minority planning an all-cloud environment.

Data reporting

With a wealth of data at their fingertips, End Users are beginning to see the operational benefits hidden within their security data; however, many cite the complexities and time consumption of data collation as significant barriers to extracting trends and insights. There's a growing need for a 'single pane of glass' approach to simplify security data management, and many End Users are hoping AI tools will help speed up the process and reduce the burden on human resources in the near future.

Current and Future State of Organizations

Key Takeaways

End Users and Channel Partners have a **growth mindset**.

Most see their organization's security efforts growing in 2024, indicating a **security-focused** year ahead.

End Users cited expansion (sites, production, and staff numbers) and upgrading existing security software and hardware as top growth priorities in the coming year.

"Expansion of production and security installation."

"Global roll out of [new systems] to replace current access control system vendors. Also expanding to locations without access control systems currently."

"Expand access to allow business units to manage hybrid working and increase occupancy levels in the offices."

Channel Partners plan growth in their client base, commercial presence, services, verticals, and geographic regions.

"Strengthening new verticals and diversifying service offerings."

"Getting more customers on board… and integrating with more systems."

"Expand and develop new clients and support existing clients."

"Increase commercial presence."

The sentiment of growth was also echoed by Consultant and Technology Partner participants.

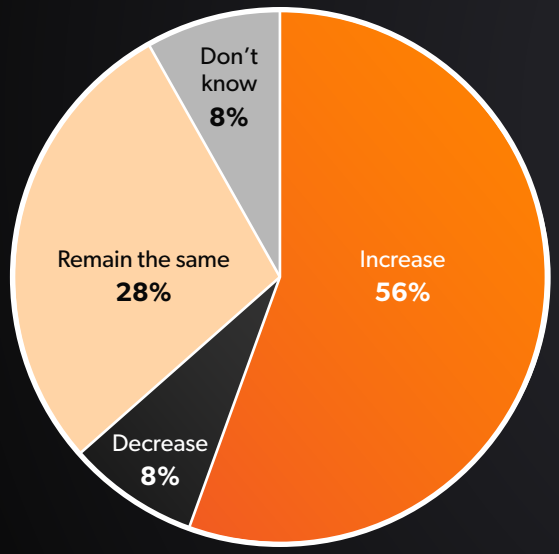
"Expansion of services across the group. Greater market share and reputation for quality."

"Continue to grow and provide independent expert security advice to our clients."

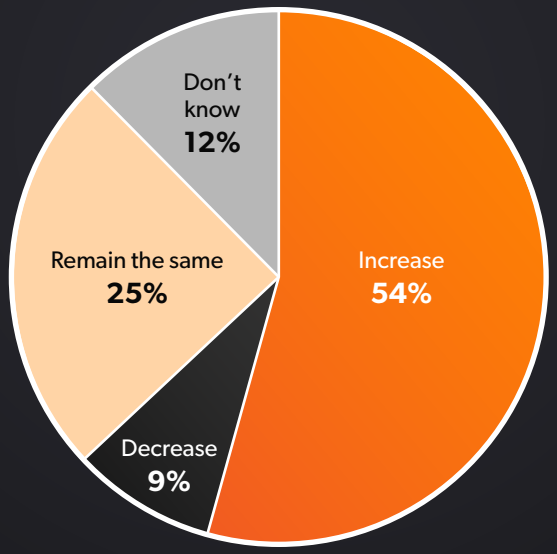
Key Takeaways

Security budgets and investments are predicted to increase

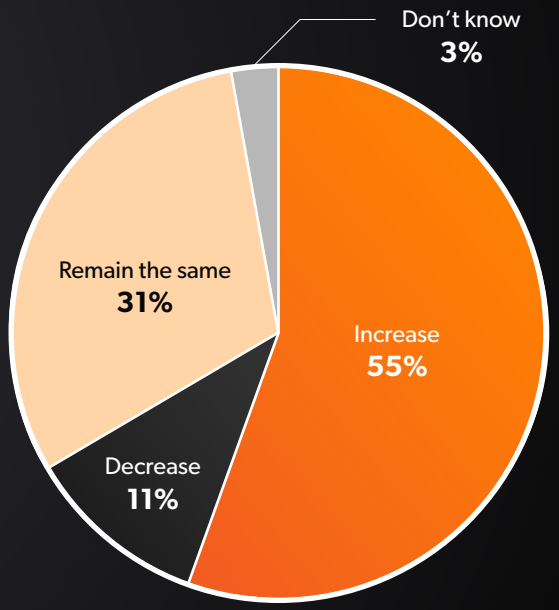
The growth and expansion themes were backed by data received on security investment. Participants were asked to indicate whether they expected to see the security budget of their organization increase, decrease, or remain the same given the current economic climate. As noted below, most participants' expectations were that budgets would either increase or remain the same.



All Participants



Channel Partners



End Users

Key Takeaways

Additional questions targeted at understanding security-focused capabilities to be prioritized over the coming year demonstrate how budgets may be allocated.

Key investments for End Users

"CCTV expansion and security system upgrades"

"Software upgrades"

"To complete upgrading of all credentials to minimum of DESFire EV2."

"Looking to make better use of mobile credentials once all readers are compatible."

Key investments for Channel Partners

"Uplift of cyber security skill sets"

"Expansion of remote servicing capabilities"

"Driving the quality of projects and service works to provide additional value for money for our customers"

Safeguarding the Digital Frontier:

The Imperative of Upgrading Security Software and Hardware

Not a month goes by without news of a cyberattack on a business making the headlines. As of September, in 2023 alone there have been over 800 publicly disclosed global security incidents resulting in an estimated 4.5 billion breached records, significantly up from the estimated 31.5 million breached records in 2022 (Ford, 2023; Irwin 2023). And although the type of attack may vary, there's one commonality among the statistics: most are a result of legacy hardware and software.

These startling numbers paint a clear picture that upgrading security hardware and software is of critical importance for businesses around the world. The battleground of commerce and communication has shifted from the physical world to the digital world, and as technology advances, so do the methods employed by cybercriminals. In this ever-evolving landscape, security systems are the frontline of defenses, making it imperative for businesses to maintain their cyber health in the relentless pursuit of security.

The consequences of leaving legacy hardware and software in place can be catastrophic, ranging from financial losses and data theft to lasting damage to an organization's reputation.

These systems become more vulnerable to attack with each passing day because they lack robust cybersecurity measures to combat modern and escalating threats, often hosting vulnerabilities that hackers readily exploit. And as regulatory bodies and governments worldwide tighten their grip on data protection and privacy, failure to meet these evolving standards can result in significant legal consequences, including hefty fines.

Upgrading security hardware and software is not merely a matter of keeping up; it's about staying ahead of the curve. Today's cybersecurity technologies provide proactive measures to significantly enhance a business's ability to defend itself – and its reputation – against increasingly sophisticated attacks. The defenses supplied by upgraded systems are no longer an option – they're a necessity and strategic imperative. Cyber threats will continue to evolve and adapt: it's up to businesses to invest in the protection of their future.

Steve Bell
Chief Technology Officer, Gallagher Security

Prioritization of Security Capabilities

When asked how organizations plan to prioritize their security capabilities in 2024, three key themes emerged:

Integrations (particularly video surveillance)

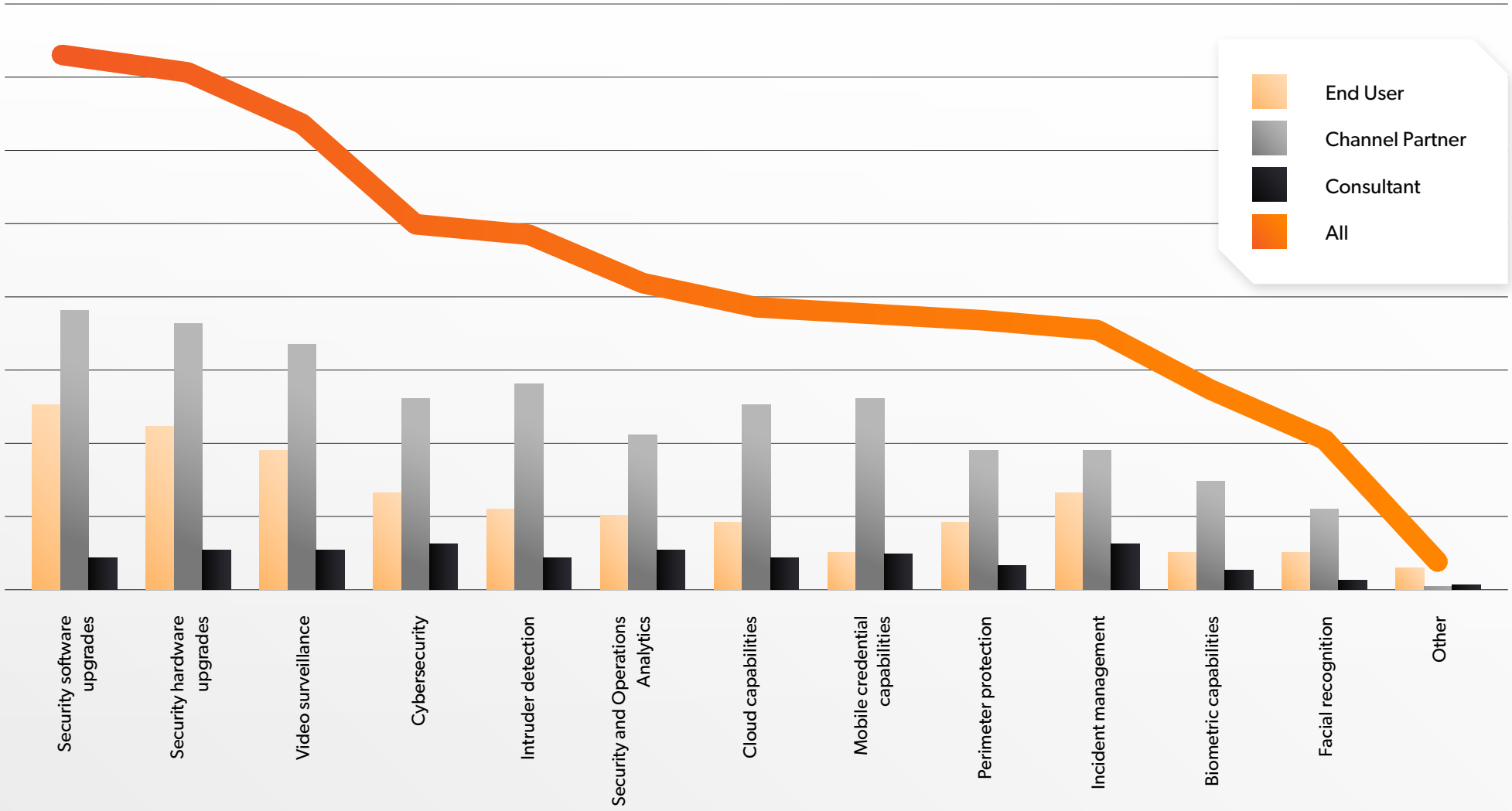
Cybersecurity

Performance and scalability

Where investments will be prioritized

The following graphic illustrates the specific system investments participants plan to prioritize in the coming year.

Prioritization of Security Capabilities



Operational Changes Due to Pandemic

The pandemic necessitated a number of operational changes to organizations around the world, including remote/hybrid working, increased hygiene caution, staff shortages, and negative economic impacts.

But when asked if the pandemic had sparked any major operational changes to participants' organizations, only a slight majority (51%) indicated changes had been introduced.

Key changes made due to the pandemic include:

End Users

- Mix between flexible and limited work from home policies (dependent on organization and role)
- More security conscious with more unmanned sites (included technical security installation to reduce physical human presence)

Channel Partners

- Fewer staff managing higher-level sites
- Reduction of staff and a switch to focus on new markets
- Working from home/remote accepted (depending on role)
- Refocus on work-life balance
- A better connectedness to the global vision
- Implementation of more digital applications

Consultants

- Heavy use of Webex video and content sharing
- Increased remote/hybrid working
- Fewer face-to-face meetings
- No longer attending client sites as frequently as pre-pandemic

The changes indicated by each group were dependent on the organization and individual roles of respondents. For example, Channel Partner Technicians, whose responsibilities include visiting End Users' sites, were unable to work from home due to the physical nature of their work.

The Cloud

Cloud solutions are here to stay, but what do the implementations and strategies around cloud deployment look like?

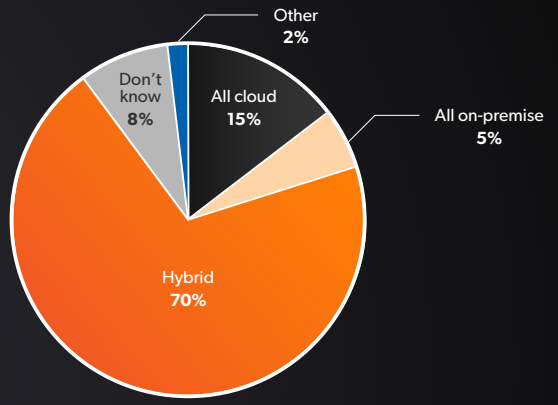
70% of participants who will be adopting cloud solutions plan to deploy a hybrid model.

End Users painted a similar picture with 69% of respondents indicating that their cloud strategy was hybrid and 11% committing to exclusively cloud-hosted solutions.

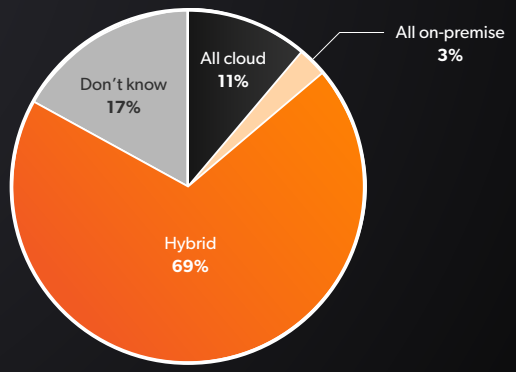
Only 3% of End Users indicated that their deployment strategy would remain entirely on premise.

However, while many security professionals have shifted opinions and are open to adopting cloud solutions, others maintain reservations and require assurance that their on-premise systems will continue to be supported into the future.

Cloud Deployment in Strategy



All Participants



End Users

Organizational Challenges

Key Takeaways

People and manpower dominate challenges.

The **growth mindset** vocalized by participants may be challenged by a perceived **lack of qualified staffing**.

Despite predicted increases in budgets, the majority of those polled identified recruitment of skilled technical staff and upskilling of existing staff as top challenges affecting organizations now and into the next year.

For Channel Partners, this may contribute to the growing emphasis on cloud solutions, which are more easily maintained and troubleshot by End Users and technicians alike and are easier to upgrade.

The Power of Training:

Bolstering Employee Retention and Tackling Skills Shortages

In recent years, it's estimated that as many as 90% of security teams have been impacted by staff shortages (Segal, 2022). Combined with the challenge of staying up to date with product and software developments while maintaining a competitive edge, many organizations are struggling to keep up with rapidly evolving security needs, resulting in knowledge gaps and increased cyber vulnerability.

But there's good news. Research shows that businesses providing learning and development opportunities experience 30-50% higher retention rates than those that don't (Lorman Education Services, 2021). And that goes for security teams, too. With 70% of employees indicating they'd consider leaving their current role to join an organization where upskilling is prioritized, the benefits of training become even clearer (Lorman Education Services, 2021).

To help our customers overcome challenges highlighted in this report, the Gallagher Security Training Team has spent the last three years innovating and reimagining our training solutions to better serve the needs of the changing security landscape.

We began with our End User Knowledge Centre platform, an educational, free-of-charge multimedia library available to our global customers, and Gallagher Care Plan, which gives those with active Software Maintenance Agreements unlimited registrations to online End User training courses at no additional cost.

Most recently, we launched our Train the Trainer program, a mentorship initiative that enables Channel Partners to deploy our Access courses within their own teams, and introduced our Virtual Classroom platform, which provides "face-to-face training" delivered by a Gallagher trainer without the need to travel. Currently, we're investing in Augmented and Virtual Reality training so we can provide "hands-on" product and skills-based training to all customers, on demand.

These initiatives have helped our customers thrive in an increasingly competitive environment, demonstrating the transformative potential of training to empower a skilled and engaged security workforce. By prioritizing continuous learning, organizations not only equip their employees with tools for success, but also build a culture that values growth and loyalty, ultimately leading to enhanced employee retention and organizational prosperity.

Danielle Mitchell
Training Manager for APAC and IMEA, Gallagher Security

Top Challenges Faced by Organizations

When asked to identify the top challenges faced by their organizations, respondents repeatedly cited ***"lack of technical staff," "lack of manpower," "keeping workforce skill level current,"*** and ***"turnover of staff and contractors"*** as major pain points, regardless of the organization's size, scope, or industry.

Beyond staffing, many End Users identified **theft** as a key challenge affecting their organization; for those in public sectors such as healthcare, education, and government, **funding** was a top problem (with those in tertiary education also identifying **low enrollment** as a challenge).

For Channel Partners, significant challenges included **security maintenance** and **software updates**, addressing **client needs and challenges**, and introducing **enhanced security technologies**. Price increases, labor, exchange rates, and overall operational costs were additionally highlighted as key pain points.

Multiple Channel Partners and Consultants also cited **supply chain delays** as continuing to be a key challenge affecting their organization moving in 2024, indicating that many security manufacturers have yet to fully recover from **disruptions caused by the pandemic** and compounded by **international conflicts**.

Security System Prioritization

Key Takeaways

Survey results revealed that End Users are placing **greater importance on physical security going into 2024**, whereas Channel Partners see **adopting cloud solutions** as a more imminent necessity.

End Users' need for **physical security prioritization** may be related to local economic drivers affecting their businesses and correlate with the frequency of **remote work** and identification of **theft** as a top organizational challenge. Conversely, Channel Partners appear to see the adoption of **cloud deployment** as inevitable and are placing greater importance on **strengthening** their cloud capabilities.

> **[Our top system priorities include] guiding clients through the transition from traditional electronic security towards more efficient task and cost solutions. This will include but not be limited to mobile credentials, cloud services, integrated authentication (single credential), analytics, and cybersecurity threats.**
>
> **Channel Partner**

A Transformative Path Forward:

Embracing the Potential of Cloud-Based Security

Of all the technologies driving the evolution of security systems, arguably none has as much potential to transform industry dynamics than the cloud, which is dramatically changing how we protect people and assets – and the foundation of how businesses operate.

Through the cloud, organizations struggling with talent shortages will benefit from teams of product and cybersecurity experts working behind the scenes (and off their payroll) to keep systems automatically updated with the latest cyber protections. Businesses looking to improve their decision-making efforts will be empowered with richer data sets, providing more nuanced insights into operations, trends, and behaviors. And with limitless potential to scale, roadblocks to growth can be removed entirely, saving time and maximizing security investments.

In short, functionalities that are simply not feasible in exclusively on-premise systems will become a reality through the cloud, whether it be a hybrid offering where customers can choose the parts of a system they manage or through a trusted vendor to manage. It isn't one size fits all, and that's the beauty of the cloud proposition.

Yet many within the security industry remain skeptical, arguing that on-premise systems offer a sense of control that the cloud simply cannot match. While this may be true for isolated use cases, on the whole, cloud solutions are rapidly evolving past initial doubts to achieve more secure, sophisticated, and robust security options.

Embracing the cloud's transformative potential requires a shift in mindset. It's not about relinquishing control, but rather adapting to a new paradigm where security is a dynamic and collaborative effort. In an era where the only constant is change, embracing innovation is the key to survival and success.

Andrew Scothern
Chief Architect,
Gallagher Security

System Integrations

Overall, system integrations ranked as the most important security system feature/technology among all participants. Top integrations identified by respondents include:

1. Video Surveillance

Video integrations were repeatedly ranked as "very important" by participants throughout the survey, with many respondents saying they're likely to invest in video surveillance (both expansion and implementation) into the year ahead.

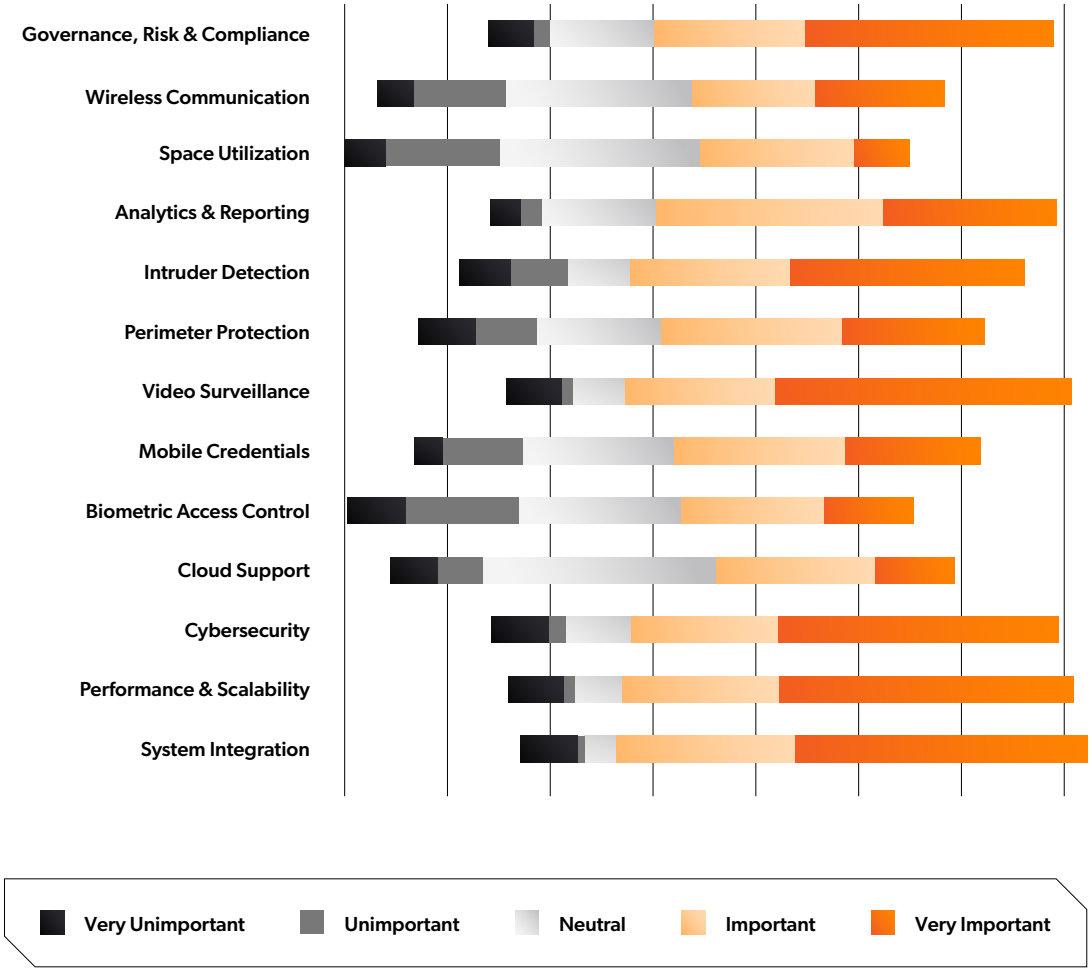
2. Identity management

e.g. Active Directory

3. Incident management

4. Data analysis

Security System Prioritization



GALLAGHER Security

Security Features and Technologies Most Important to Organizations

All Participants

System integrations

Performance and scalability

Video surveillance

Cybersecurity

Analytics and reporting

End Users

System integrations

Cybersecurity

Performance and scalability

Video surveillance

Analytics and reporting

Channel Partners

Performance & scalability

System integrations

Cybersecurity

Governance, risk, & compliance

Intruder detection

Consultants

System integrations

Performance and scalability

Video surveillance

Cybersecurity

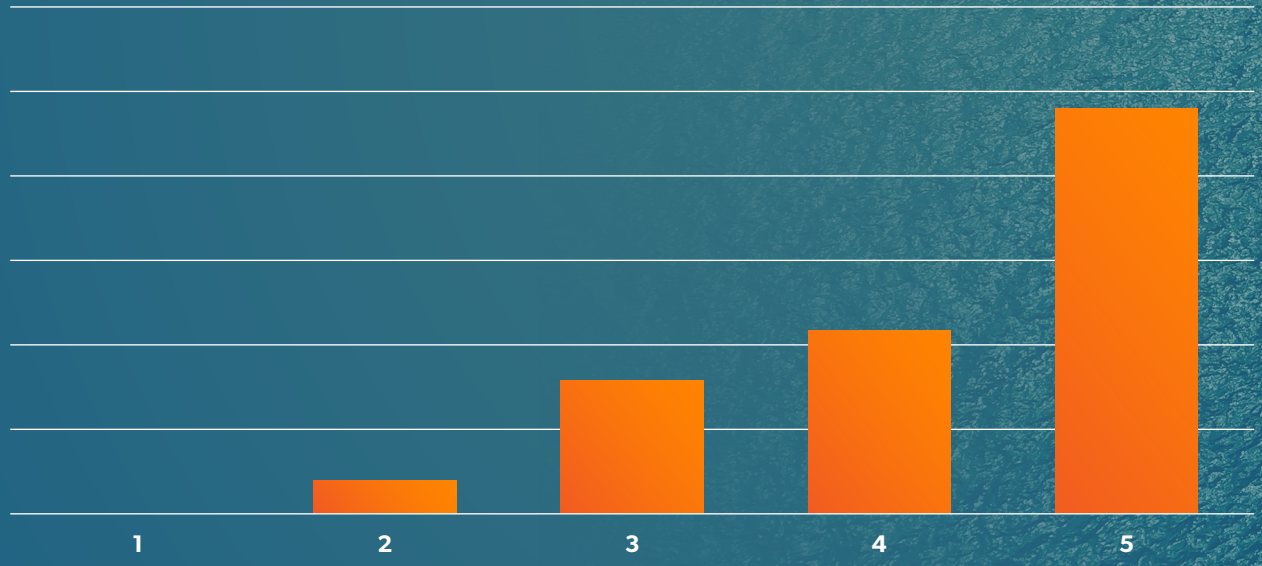
Perimeter protection

Manufacturer and Supply Chain Visibility

When asked to rank the importance of supply chain visibility from security manufacturers, participants indicated that knowing where materials are sourced from is of high importance for businesses. On a scale of 1-5, where 1 is not important and 5 is very important, **the overall ranking for supply chain visibility was 4.26.**

As Channel Partners and Consultants continue to say they're impacted by supply chain pressures, it's likely many are inspecting their security vendors' production habits more closely, a trend likely to continue beyond 2024 as standards shift towards visibility.

On a scale of 1-5, how important is it that your security manufacturer provides visibility on where their materials are sourced from?



Importance of Cybersecurity

Key Takeaways

Recognition is growing that **strong cybersecurity defenses are critical**, but help is needed to understand best practices.

Help is needed to meet growing demand for best cybersecurity practices.

Across the board, participants said they recognized the need to **strengthen and diversify** their cybersecurity implementations, though many cited the **lack of skilled staff and general education** on the subject as pain points standing in the way of achieving their goals.

Setting a Higher Standard:

Fortifying Cybersecurity to Face the Unknown

Cybersecurity and physical security are often inherently linked to one another: it's difficult to have a secure physical solution without considering elements of cybersecurity, and impossible to avoid physical components within a cyber-secure environment. It's becoming increasingly important for businesses to consider both to achieve a holistic security solution.

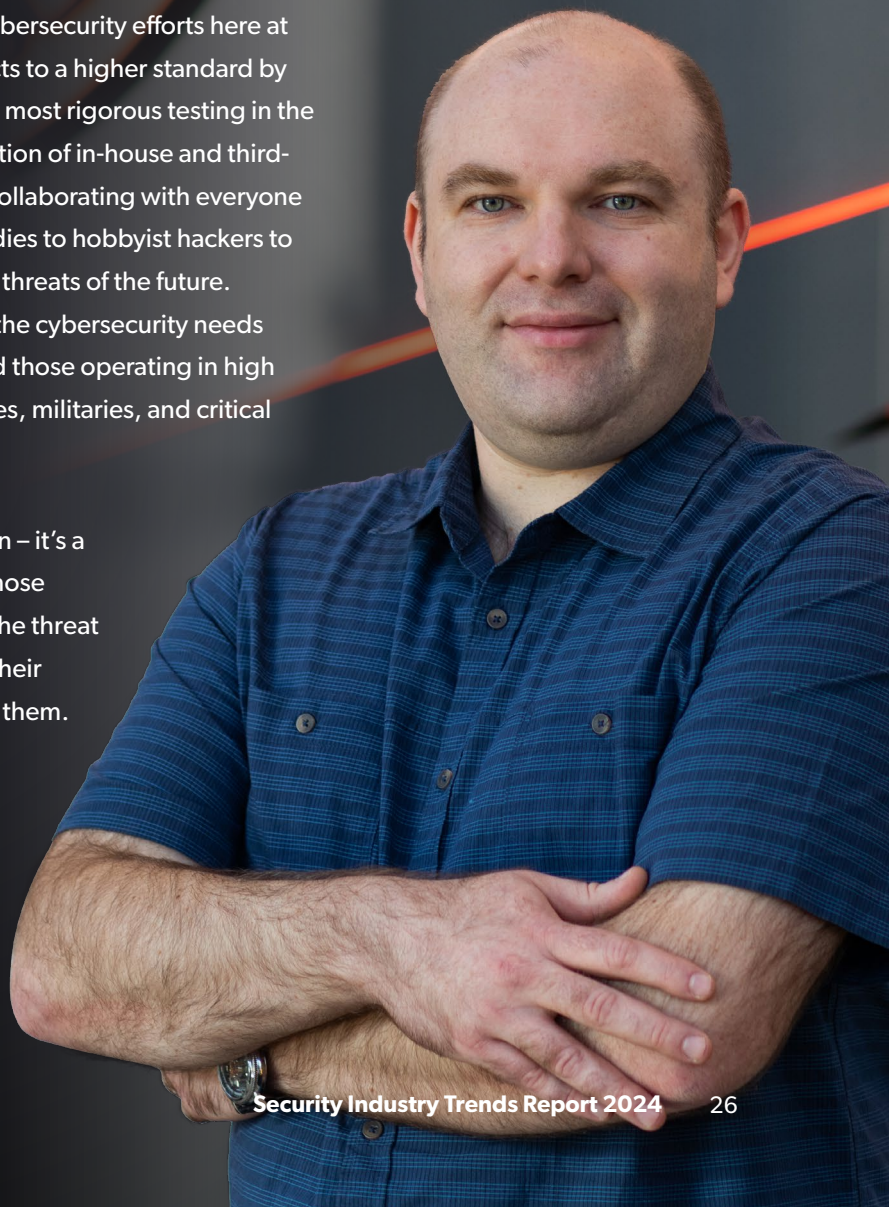
Highlighting the critical link between the two is the rise of cyber-physical attacks, where physical losses are enabled by cyber breaches that prevent systems from altering the event. Such attacks blur the lines between the physical and digital, raising new questions in their wake. For example, if an organization carries both theft and cybersecurity insurance, where does the liability lie in the event of a cyber-physical attack? Most insurance providers require the installation of an alarm system for theft coverage, but if that system's alarms were disabled due to a cyber attack, who's responsible?

Fortunately, I've not seen widespread attacks of this nature – often, they're just proof of concept in test labs. But as time marches on, I do expect these combined arms attacks to make their way into the corporate arena. We've already seen some of it with access card cloning, and there's more to come.

Threats like these inform our cybersecurity efforts here at Gallagher. We hold our products to a higher standard by subjecting them to some of the most rigorous testing in the industry, employing a combination of in-house and third-party penetration testing and collaborating with everyone from standards accrediting bodies to hobbyist hackers to fortify our solutions against the threats of the future. As a result, our solutions meet the cybersecurity needs of both commercial entities and those operating in high security, like government bodies, militaries, and critical infrastructure sites.

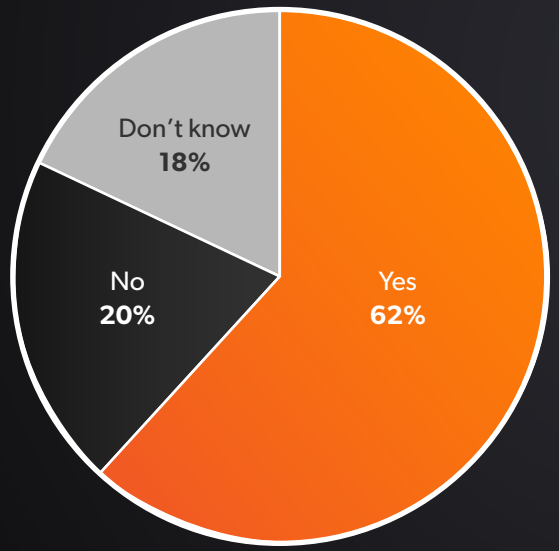
Cybersecurity isn't a destination – it's a continuous journey, and only those prepared to evolve alongside the threat landscape will be able to take their customers on that journey with them.

Rob Cowsley
Security Architect (Cyber),
Gallagher Security



Implementing New Cybersecurity Capabilities

In the past year, 62% **of respondents** said that they had implemented new cybersecurity and/or data protection capabilities in 2023.



53% **of End Users** said they had implemented new capabilities such as:

"Enhanced server scanning and controls, east-west network lockdowns, improved software computer email scanning and enhanced software activity scanning."

"Password management, logs management, patching management, penetration tests and phishing awareness"

"Fully implemented application control for all devices. Additional DPM addressing email and cloud exfiltration of data. Remains work in progress."

"Upgraded security"

Implementing New Cybersecurity Capabilities

60% of Channel Partners also noted the organizations they work with had implemented new capabilities over the past year, including:

Password management

"Internally: increased use of password management tools; 2FA; Externally: addition of new security to help to protect data"

"Increase password [complexity], using upper and lowercase and increase the amount [of characters] from 12 to 16"

Firewalls

"Fire wall as a service moving the client's security off of production network to a private security"

"Firewalls & resilient password policies"

ISO 27001 accreditation

Several participants plan to create **dedicated cybersecurity positions** within their organization in 2024.

"Hiring of cybersecurity consultants to understand risk and train staff"

Channel Partner

"Cyber department formed"

End User

Unlocking the Potential of Data and Analysis

Key Takeaways

End Users see great potential to tap into their **security data**.

With a wealth of information stored within their security systems, End Users are increasingly eager to extract **data that helps strengthen and streamline their operations**; however, with **limited human resources**, many hope AI tools can help their organization reduce the time commitment and complexities inherent to data management.

Making Data-Driven Decisions Through Access Control

Modern access control systems have become so much more than stand-alone products securing doors: they've evolved into sophisticated ecosystems providing not only enhanced physical security, but the kind of operational insights critical for making better decisions - and all through a single user interface.

At the center of these connected systems are integrations, the importance of which can't be overstated for businesses today. In fact, they've become so important that integrations with electronic access control systems are no longer optional – they're a necessity.

That's because integrated access control systems provide a rich set of data that organizations can tap into for better decision-making and operational improvements. By analyzing access patterns, businesses can optimize workspace utilization, improve individuals' experiences to increase employee retention, and even enhance productivity.

For example, understanding peak arrival/departure times and pinpointing access bottlenecks can help businesses adjust staffing levels and coordinate smoother hours of operation. Occupancy and space utilization can be monitored to help understand how buildings are being used and improve office configurations. Integrating with building automation systems can optimize energy usage by adjusting lighting, heating, and cooling based on occupancy data, reducing costs and contributing to sustainability efforts. And so much more.

As technology continues to advance, we can expect even more seamless and intelligent integrations.

Businesses investing in electronic access control systems must prioritize integrations to grow with their organization's needs and equip themselves for navigating the complex security – and workplace – landscapes of the future. Because in the end, it's not just about controlling access: it's about making better decisions that keep people at the heart of everything you do.

Scott Ridder
Value Stream Lead,
Gallagher Security

Intelligence Through Data

There is a real and growing need in the market for the collation, reporting, and analysis of data to aid in decision making, identification of trends and anomalies, and predictions of vulnerabilities within organizations.

In fact, the big data analytics market is expected to grow at a Compound Annual Growth Rate (CAGR) of 15.3% to reach $638.66 billion USD globally by 2028 with the software segment responsible for driving most of the growth, demonstrating the increasing need for effective data management solutions (The Insight Partners, 2022).

When asked which aspects of their organization respondents hoped to improve through the analysis of security data, four key trends emerged:

1. **Occupancy rates:** Respondents want to improve their understanding of occupancy rates throughout their sites, including the flow of foot traffic, time spent per room, and the movement of people across facilities.

   A Channel Partner respondent noted that access to this data resulted in low usage spaces being repurposed; another noted it helped their health and safety team manage desk occupancy.

2. **Utilization of resources:** Participants also expressed a desire to understand how their organization's resources were being utilized for the purpose of identifying upward trends, enabling them to better manage resource allocation and budgets.

   An End User in the education industry noted that in addition to enhancing the management of resources, these insights would also benefit their TEFMA reporting (Tertiary Education Facilities Management Association) and facilities management benchmarking. Others cited the benefits of understanding the utilization of hardware to predict maintenance and lifecycle management as a need within their organization.

3. **Identifying vulnerabilities:** A theme emerged about the use of data to identify vulnerabilities and mitigate risk among respondents. In particular, organizations are turning to security data to determine:

   - The physical security of buildings
   - Whether compliance standards are being met
   - Where weaknesses exist within their systems
   - If equipment or communication faults are present
   - The extent of their door traffic

   Additionally, understanding incident history helps organizations forecast potential threats and employ preventative measures.

4. **Trend, behavior, and anomaly identification:** Many respondents said they require a 'single pane of glass' view of data that provides full visibility over a range of their organization's activities for the purpose of identifying trends, common behaviors, and anomalies. Through a consolidated view of data, participants hoped to answer questions like:

   - What are the trends in system usage that can inform where budget and resources can be invested?
   - What are the atypical behaviors being identified and how can we address them?
   - How are groups and individuals behaving on site, when and how long are they present, and what activities are they engaging in?

The adoption of AI

AI is expected to see an annual growth rate of 37.3% from 2023 to 2030, with 25% of companies currently reporting reliance on AI for operational optimization and to compensate for understaffing, a pain point repeatedly identified by survey participants (Haan, 2023).

Several participants noted that they saw great potential for AI to improve data management processes, like the consolidation, collation, and evaluation of raw data. The following illustrations outline the key impacts respondents believe AI will introduce to their organization:

However, many said they remain unsure of the impact AI will have on their organization going into 2024. In a recent survey of business owners, 35% questioned whether their staff had the necessary technical skills to use AI tools effectively; with many End Users and Channel Partners reporting similar concerns about technical skills, it's possible the lack of training on AI technology may be affecting respondents' willingness to embrace these tools or see their benefit (Haan, 2023).

The Importance of Listening:

The Customer as Compass

I've worked with product teams across different industries and countries, and while each has countless tools for product development, I've found nothing to be more imperative than the simple skill we're taught to practice as children: listening.

Listening is more than a customer service exercise - it's a strategic necessity to guide the development of solutions that solve real-world problems. When done with intent, it fosters the kind of foundational trust and loyalty that long-lasting partnerships are built on.

But listening is not a passive activity. Understanding customers' expectations and day-to-day security concerns requires active and ongoing engagement to keep up with the evolving needs, pain points, and requirements across their various industries.

At Gallagher Security, our customers are our compass. As a privately-owned company, we're committed to reinvesting 15% of our annual revenue back into our research and development each year, empowering us to be customer obsessed in everything we do. The stories and insights within this report are the kind that steer our direction and ensure our decision-making process is innately customer led.

Staying at the forefront of innovation and customer-centric solutions is the foundation of sustained success. Listening to customers and using research to inform our product development positions Gallagher to not only adapt to shifting needs, but to forge a path toward a more secure future. We hope the insights contained within this report can do much the same for you and your organization.

Meredith Palmer
Chief Product Officer,
Gallagher Security

References

Conerly. B. (2023, August 5). Recession Forecast Still Right For Late 2023 Or Early 2024. Forbes.

https://www.forbes.com/sites/billconerly/2023/08/05/recession-forecast-still-right-for-late-2023-or-early-2024/?sh=513144c55cf1

Ford, N. (2023, October 5). List of Data Breaches and Cyber Attacks in 2023. IT Governance.

https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

Haan, K. (2023, April 25). 24 top AI statistics and trends in 2023. Forbes.

https://www.forbes.com/advisor/business/ai-statistics/

Irwin, L. (2023, January 3). List of data breaches and cyber attacks in December 2022 – 31.5 million records breached. IT Governance.

https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-december-2022

The Insight Partners. (2022, May 24). Big data analytics market is expected to reach US$ 638.66 billion by 2028. [Press release].

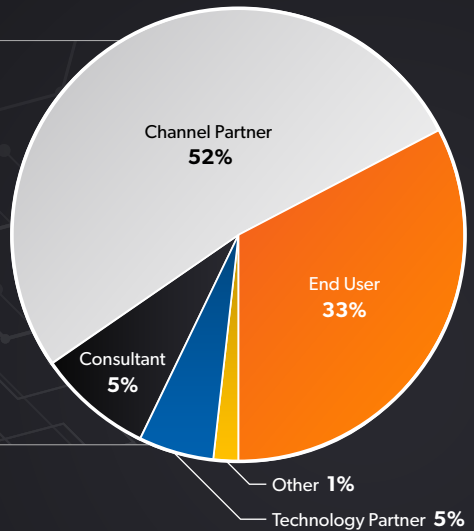
https://www.theinsightpartners.com/pr/big-data-analytics-market

Methodology and Demographics

Methodology and Demographics

Participant Overview

From July 3 to August 31, 2023, Gallagher Security surveyed global security professionals with the intent of understanding the future of their organizations and stakeholders and what they perceive as the most important issues relevant to their security systems in the year(s) ahead. Surveys were distributed to End Users, Channel Partners, Consultants, and Technology Partners across Oceania, North America, Europe, Asia, and Africa.



Number of Employees by Group

End Users

67% of participants had 1,000+ employees within their organization.

Channel Partners

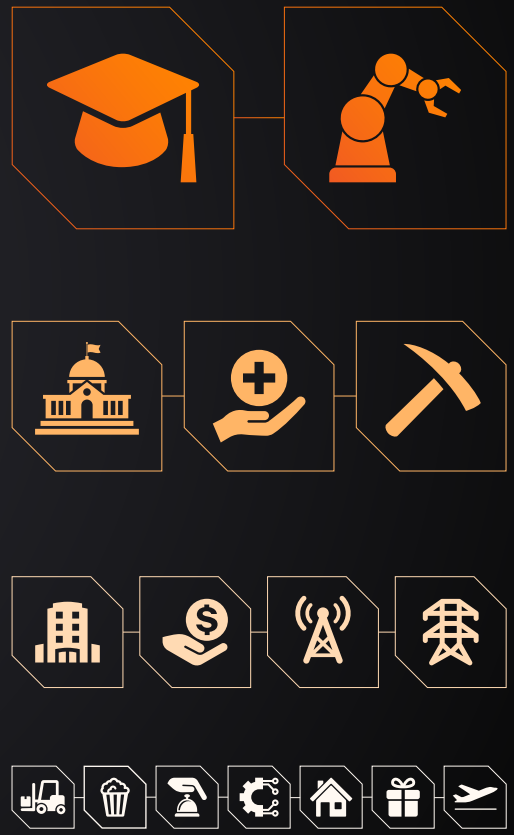
More distributed on the smaller size with **86%** of respondents working in organizations with 500 employees or less.

Consultants

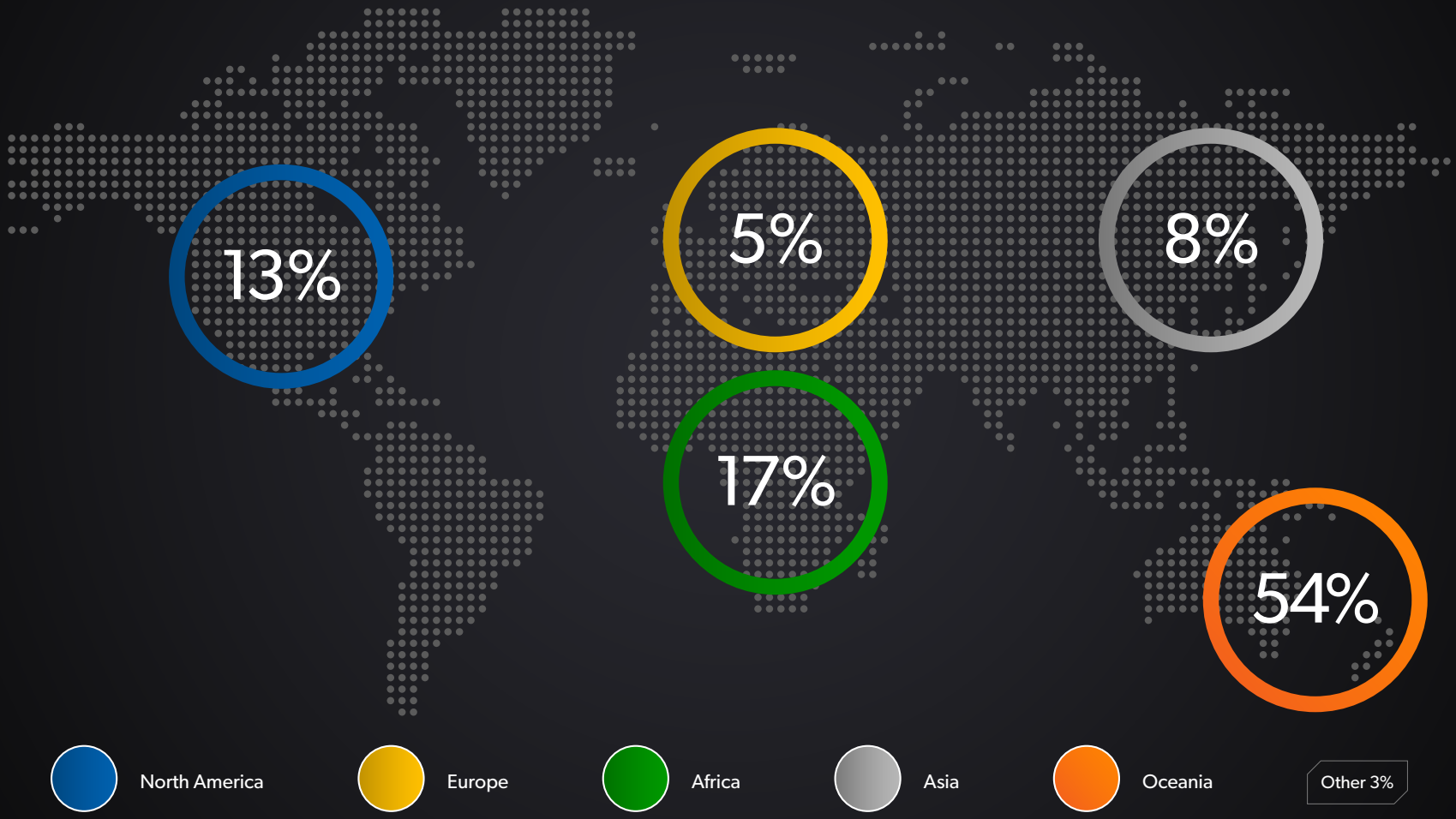
Majority **78%** of consultants worked in organizations with 1-20 employees.

End User Vertical Representation

- Education
- Manufacturing
- Government
- Healthcare
- Mining & Resources
- Commercial Buildings
- Financial Services
- Communications
- Utilities
- Distribution & Logistics
- Entertainment
- Hospitality
- IT Services
- Residential
- Retail
- Transportation



Respondents by Global Continent



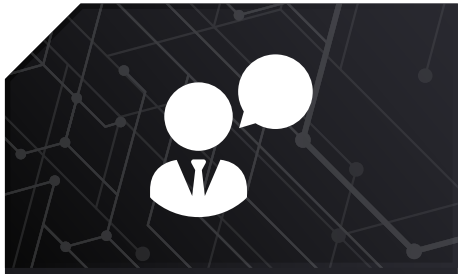
Participants' Roles

End Users

- Security management
- IT management
- Control room
- System maintenance and support centric
- Building/facilities management
- Essential systems management
- Engineers

Channel Partners

- Executive-level roles (ie: CEO, president, director, etc.)
- Specialists/engineers
- Technical lead/director
- Technicians
- Project managers
- Sales/business development managers



Consultants

- Executive-level roles (ie: president, principal, director, etc.)
- Owners
- Miscellaneous leadership roles

Technology Partners

- Senior/lead technician
- System engineer
- Project manager
- Installation/support technician

About Gallagher Security

Gallagher Security is a global leader in integrated technology solutions that helps organizations around the world protect, secure, and manage people and assets. Our award-winning solutions are trusted by government, defence, commercial, industrial, healthcare, transportation, mining, and educational organizations in 140 countries.

Gallagher designs and manufactures a comprehensive suite of security software and hardware - including integrated access control, intruder alarm, and perimeter solutions – all on site at our global headquarters. The intelligent technology can be scaled and customized to deliver business efficiencies across simple, enterprise, and high security sites.

Trusted by over 15,000 security customers worldwide, Gallagher solutions are used to simplify life on campus within the education sector, keep staff and patients safe in healthcare, ensure the highest security requirements are met for government sites in the Five Eyes alliance, safeguard critical infrastructure within the utilities industry, and ensure uninterrupted movement for transport and logistics.

Visit security.gallagher.com to learn more

security.gallagher.com

Gallagher World Headquarters 181 Kahikatea Drive, Melville, Hamilton 3204, New Zealand **Phone** +64 7 838 9800 **Email** security@gallagher.com