psacertified™

2022 Security Report

The Turning Point for IoT Security

2022: The Year of Change

Table of Contents

Introduction

By 2025 it is expected that there will be around 55.7 billion connected devices which will influence the lives of the global population daily. The scale of these connected devices – and the rate they are growing – will continue to shape our present and our future.

Underpinning this wholly connected world is the Internet of Things (IoT), and it is poised to have an impact on the decade ahead few would have ever imagined. We have moved beyond the stage of early adopters towards the metaverse, a truly digital-first decade in which interactions with the physical world are primarily digital. We can share, work and live connected lives like never before, all made possible by processing data at the edge. The digital world unlocks innovation, including the complete digitalization of the home, office, city, industrial IoT, transportation and manufacturing.

With this in mind, the challenge of IoT security is sharply coming into focus and the World Economic Forum now lists cybersecurity failure as a critical threat in the next two years. Following our inaugural PSA Certified Security Report last year, we felt it necessary to review what progress has been made and what is needed to protect products and systems from adversaries in the long term.

The findings of this report show that 2022 will be a turning point where security is no longer a secondary concern. It will become proactively placed center of any IoT strategy, whether you're buying devices or making them. The results demonstrate that the industry has recognized the need for independently evaluated, ubiquitous security. They prioritize IoT security, highlighting a universal desire to build a more secure IoT ecosystem to deliver assurance and allow deployments and services at scale. And while the rate of IoT security adoption has historically lagged behind the pace of digital transformation, there is now an industry-wide imperative to rectify this.

What's more, we will see trusted components, those with a Root of Trust (RoT), being actively procured and positioned as the foundation of IoT security. Through their adoption of the RoT, the IoT ecosystem will take the first steps to a more secure IoT.

Our intention with the PSA Certified 2022 Security Report is to give you an insight into the current state of play in IoT security, what is transforming and what is needed from everyone to make the IoT more secure. Join us as we explore the data in more detail, along with the knowledge of our founders and partners, plus a variety of external data points.

David Maidment

Senior Director, Secure Device Ecosystem, Arm
(one of the PSA Certified co-founders)

About PSA Certified

PSA Certified is a global partnership of security-conscious companies who are proactively building security best practices into devices at scale. Our security framework and independent third-party evaluation scheme was originally spearheaded by Arm, CAICT, ProvenRun, Riscure, SGS Brightsight, TrustCB, and UL. Today, the original founders alongside new members, Applus+ Laboratories and ECSEC Laboratory, are providing the resources needed to build a security by design scheme that starts with the Root of Trust and is aligned to cybersecurity requirements of USA, Europe and China.

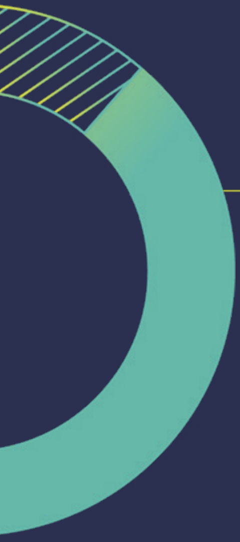
PSA Certified has scaled to become one of the fastest growing, most valued security ecosystems, globally. Being awarded 'Ecosystem of the Year' in the IoT Global Awards 2021 is testament to the role it has played and will continue to play, in uniting industry, standards bodies, regulators and insurers together under one initiative. In doing so it's accelerating the cross-industry collaboration required to untap the full potential of the IoT.

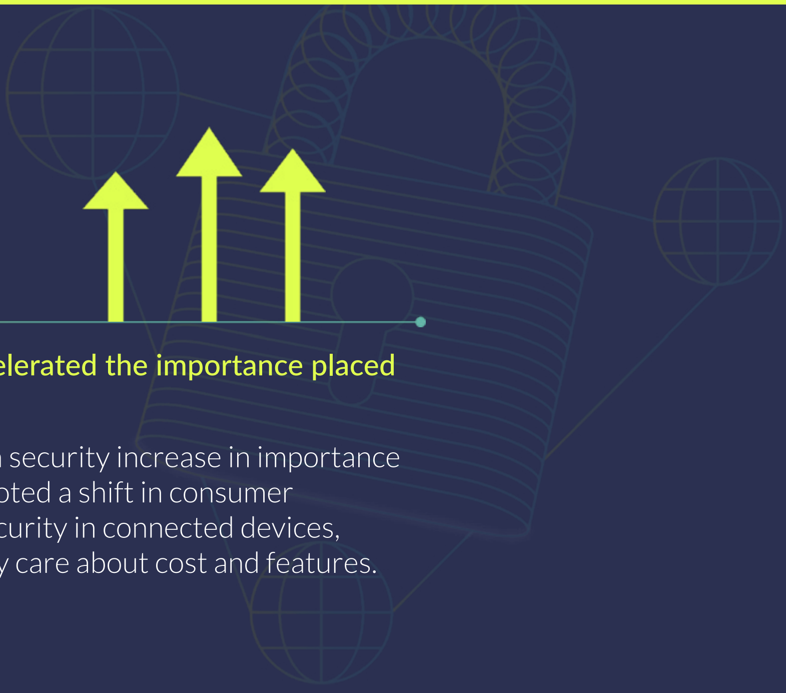
With nearly 100 certifications from over 50 partners, PSA Certified has democratized the adoption of security across the electronics industry, giving the ecosystem the confidence to innovate, while protecting consumers, businesses and service providers from the most common hacks.

FIND OUT MORE

Executive Summary

The PSA Certified 2022 Security Report, gathered from the survey of 1,038 technology decision makers, reveals that the direction of travel is clear: best practice security is no longer optional. It must be integrated into every connected device, process, company and culture.

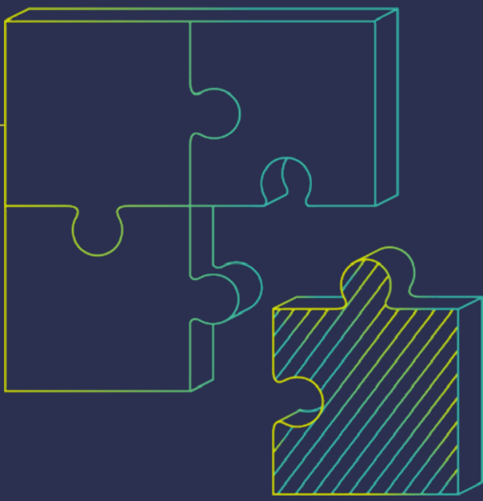




90%

Digitization and cyber threat have accelerated the importance placed on security:

90% of respondents surveyed have seen security increase in importance over the last 12 months. Respondents noted a shift in consumer perspective to prioritize checking for security in connected devices, debunking the myth that consumers only care about cost and features.



96%

The desire for best practice guidanceis higher than ever:

96% of those who responded to our survey said they would be interested in an industry-led set of guidelines on IoT best practices - a considerably higher finding than the 84% of respondents in our previous survey.

9 out of 10

Building a security-first culture is no longer the domain of the few, but the many:

almost 9 out of 10 respondents agree that security is a top 3 priority for their business (88%), and it has increased as a business priority in the past 18 months (81%). The highest priority was ensuring there is a “security first” culture in the company (42%).

83%

Expectations around security are growing exponentially:

83% of respondents look for specific security credentials when buying connected products as a consumer, and 76% look for them when buying on behalf of their company; 68% of this total admit that while they value security credentials when buying for their company, they don't know which to look for.

96%

Security drives commercial value:

96% of respondents believe having security in their products positively impacts their bottom line. This can come in many forms, from the ability to deliver true differentiation in their product lines, to creating premium products tailored to a more sophisticated marketplace.

94%

Lack of expertise as a barrier:

94% of respondents are at least somewhat satisfied with the level of security expertise within the employees in their company, but only 31% are very satisfied, highlighting that lack of in-house security expertise can still be considered a barrier. The World Economic Forum estimate that there is a gap of more than 3 million security experts worldwide.

95%

Certification underpins a more secure IoT:

Despite cost being a perceived barrier, 95% believe that if the industry increased its rate of certification, it would only be beneficial. This momentum towards security certification will accelerate the path to a more robust IoT ecosystem.

The findings of this years report highlight that while awareness around security is gathering pace, there is still a great deal to be done around education and delivering best practice. Presently, there is no single-sized solution to the challenges being faced by the industry, but there is a growing desire, and need, for a collaboration-based framework – such as the one crafted and guided by PSA Certified.

Security as a Priority

Executive Summary

Our last report outlined that although the ecosystem viewed security as necessary, the industry was still on the brink of a transformation. It was ready to make that leap of faith but had yet to spring into action. Today, we are seeing an industry with one foot already off the diving board, with the final hurdle towards a perfect dive being around collective action.

When we consider IoT security, we refer to products, services, and platforms designed from the ground up to be secure from cyber-attacks. It is becoming a priority for countless industries and businesses. Increasingly, enterprises are waking up to the commercial and practical benefits of IoT security, while their users, partners and employees are increasingly starting to ask for it. The economy is ready for IoT security to be the norm.

Our survey found that 4 in 5 respondents agree that security has increased as a priority over the past 18 months, largely due to regulatory pressure and consumer demands. Over a third believe distributed working and the pandemic have increased the likelihood of IoT hacks, with 17% of respondents citing they had been the personal victim of an IoT hack, and 22% of companies they work for suffering similarly. There is also a recognition that security adds value to products, with 69% agreeing that you can potentially charge a premium for products with security built-in as it increases trust and helps technology to scale faster.

Finally, building on the PSA Certified Security Report 2021, we're seeing that the importance of the Root of Trust and trusted components continues to increase across the ecosystem.

> "Arrow Electronics' knows the importance of designing with security in mind to protect customers' data and IP. Arrow is collaborating with PSA Certified to provide certified platforms that align with cyber-security standards, using trusted silicon and offering engineering services to get to market faster and more securely."
>
> **Aiden Mitchell**, Senior Vice President,
> Global Marketing & Engineering, Arrow Electronics

The State of IoT Security Today

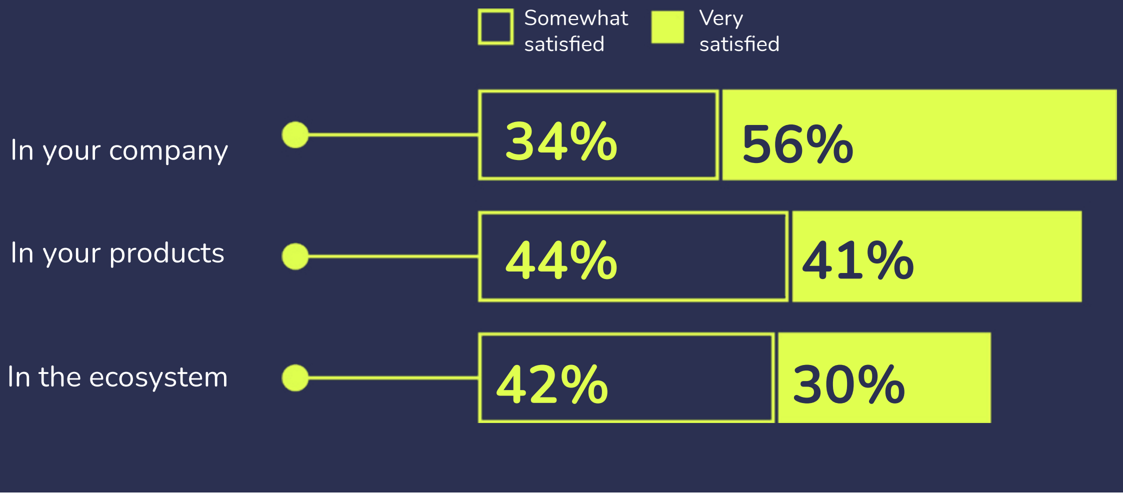
With IDC predicting that by 2025 there will be 55.7 billion connected devices worldwide, the need for IoT security has never been more pressing. But the cost of IoT insecurity when designing products is higher than it has ever been. According to analysis from cybersecurity provider Kaspersky, the first half of 2021 saw 1.5 billion attacks on smart/IoT devices - double the number from the previous half-year – while the impact of the cost of cybercrime is predicted to reach $10.5 trillion by 2025 (source: CyberSecurity Ventures).

This year, our research revealed that 22% of respondents worked for companies that had been victims of hacks due to vulnerabilities in third-party products or services. In comparison, 20% have sold products that have been used as a hacking vector or weakest link into customer systems.

At the same time, digital transformation is ever-evolving. We're scaling deployment and the number of connected devices at an incredible rate, fueled by advancements in technology such as 5G and Wi-Fi 6 that will improve user experience and encourage further adoption.

Whatever the connection, or the means of delivery, the connected future is about deploying digital services at scale. Establishing trust in those devices, the data and the services that come from them is mission-critical and building services based on insecure devices is not an option. Security-related concerns, product vulnerabilities and cybercrime, were cited within the top three risks to successful deployment of digital transformation. IoT security must be designed and implemented from the ground up, and the industry is fast aligning on its importance.

How satisfied are you with the quality of IoT security implementations in these scenarios?



> "Today's security gaps are exacerbated by the seeming lack of "defence-in-depth" in products, which provides layers of security to not only mitigate threats today but also layer on techniques to isolate vulnerabilities that arise in the future. Shifting focus to deploy defence-in-depth from the silicon and extend throughout devices, will help future proof product security decisions made today."

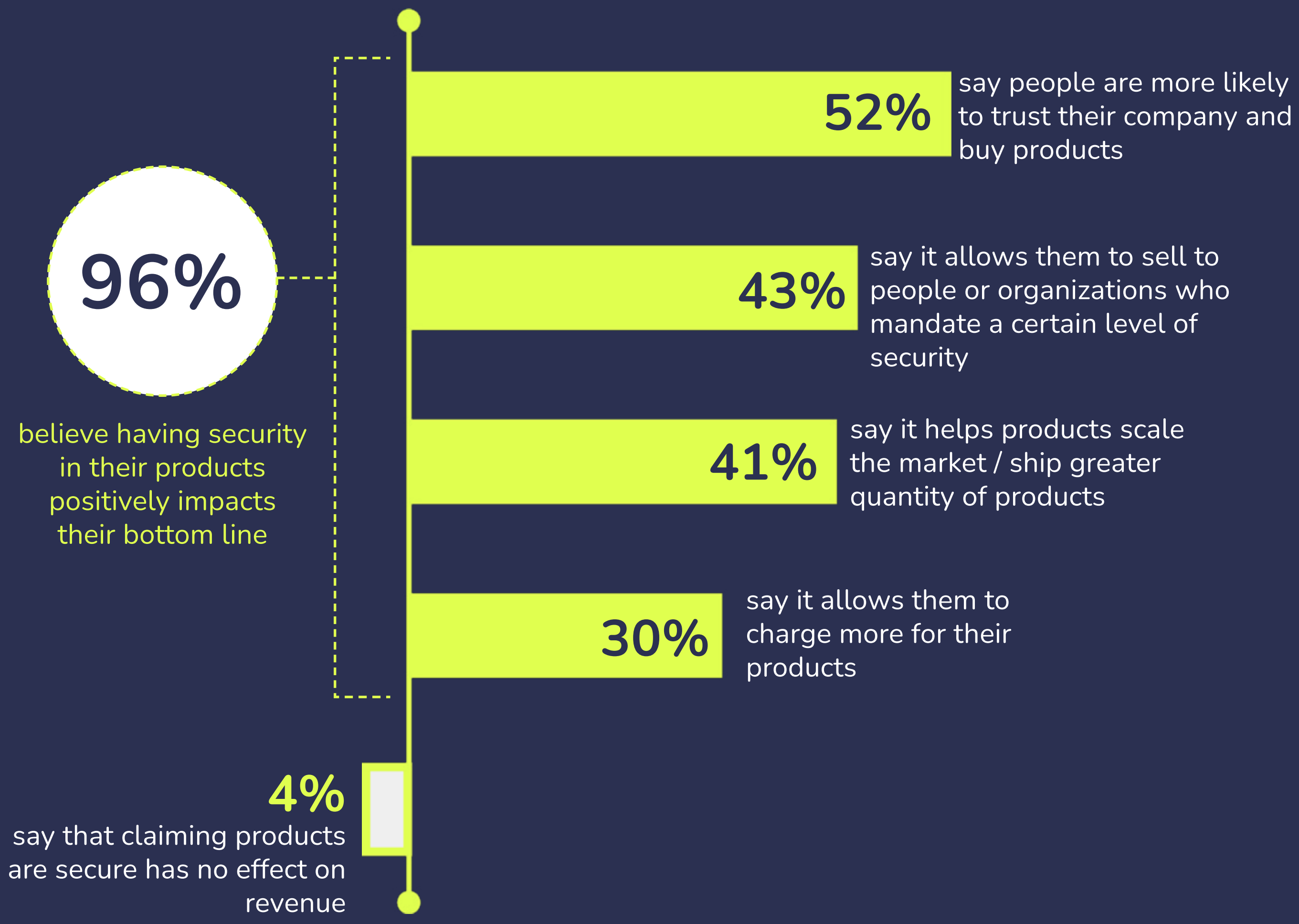
Erik Wood, Director of Microcontroller Security, Infineon

The Benefits to IoT Security Implementation

IoT security does not just protect the end-user. From our research, respondents almost unanimously agreed (96%) that having security in their products makes a positive impact to their bottom line. Product differentiation and charging a premium is tempting to any business. But being able to ship more significant volumes of products because partners and end-users trust them, and delivering them to the market at speed, is also a key advantage.

Our survey respondents see that IoT security could also reduce future costs (31%) and reduce insurance premiums (20%). Furthermore, 69% agree you can charge a premium for products with specific security credentials, and 72% are willing to pay such a premium. From a financial perspective, the proof is there to see.

96% believe having security in their products positively impacts their bottom line



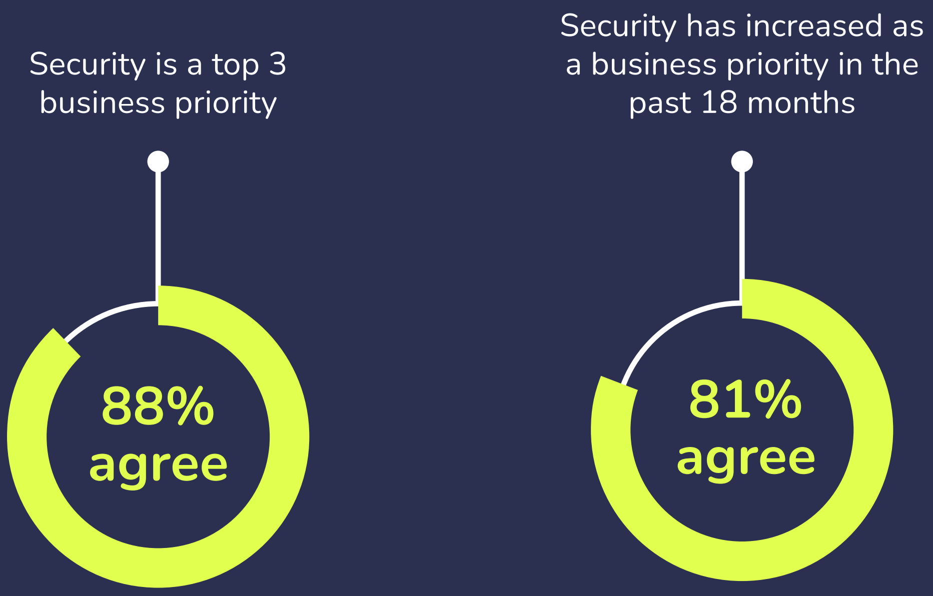
Q. Do you believe that having security in your products positively impacts your bottom line? (All that apply selected)

With attention growing around hacks and vulnerabilities, it is no surprise that our survey found that security is now a business priority. 88% of respondents cited that security is a top-three priority in their business.

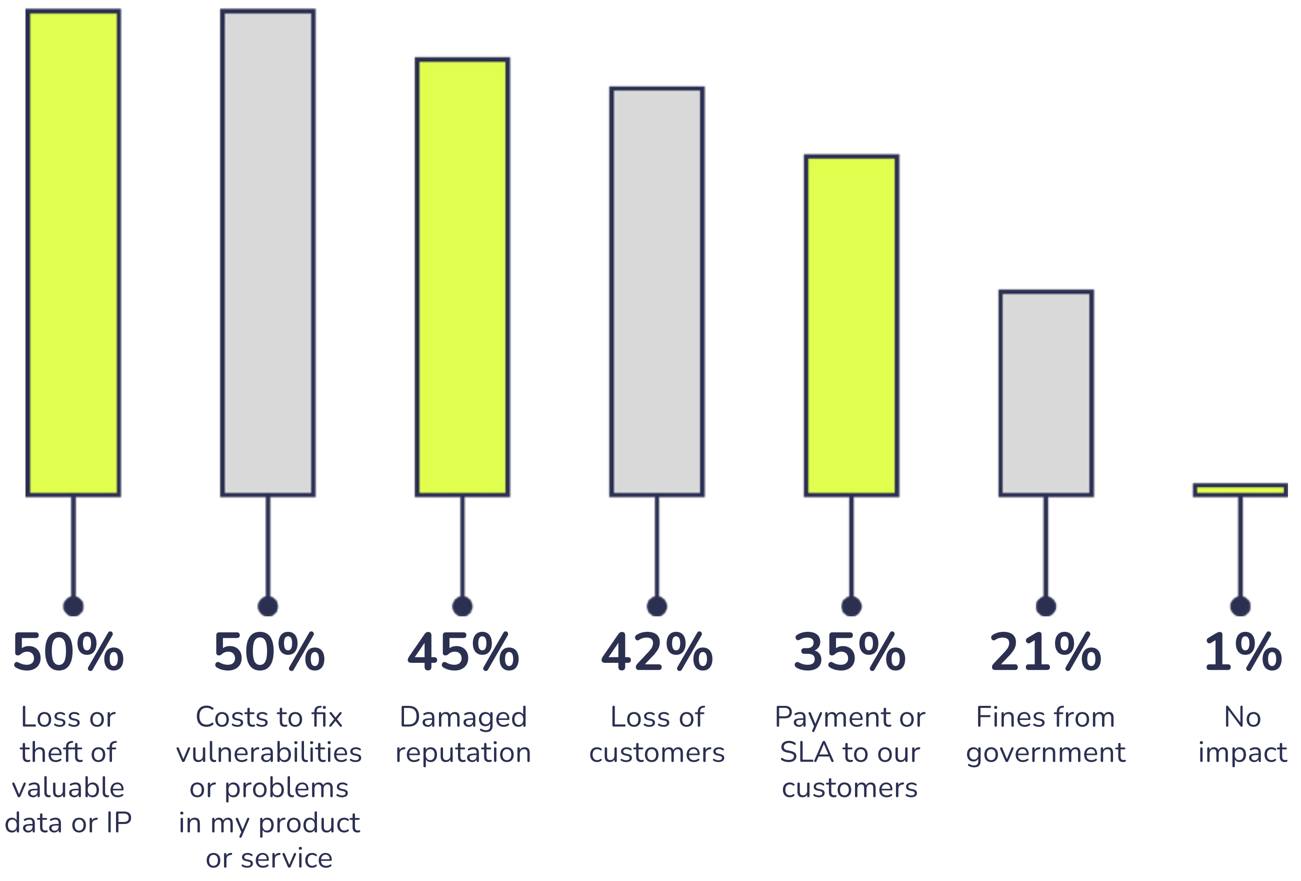
There is no disagreement that the industry is heading towards a digital-first decade, with rapid digital transformation underpinning everything we do. However, 34% of respondents believe that digital transformation is moving faster than IoT security, with silicon vendors, software providers and cyber insurers the most likely to agree with this.

As we reach the turning point of IoT security, we must avoid the past pitfalls, where security lagged behind the pace of digitization and technology. We can overcome security challenges through the democratization of security, through an agreed and applied framework.

When considering the priority your business places on security, please let us know to what extent you agree or disagree with the following statements



99% of respondents agree that there are serious consequences for a business following a hack:



Q. What do you think the impact of a hack would be on your business? Select all that apply

The Importance of the Root of Trust

Increasingly, we are seeing consumers and businesses look for devices built on the Root of Trust (RoT). A RoT built into the silicon, containing all the critical security features, will become a necessity in many areas of standards, compliance, and regulation and is seen as the starting point for devices built from the ground up with secure components. Specifically, the RoT is the part of a processor where all secure operations are performed making it a trusted component – on which IoT security is founded.

Our report found that trusted components were growing in importance with IoT decision-makers. In fact, of those surveyed, 68% recognized trusted components as essential options for creating secure devices. Notably, the RoT adoption rates are even higher in critical markets such as health monitoring (78%) and industrial (also 78%), where protecting data, and in some cases individuals, are such a vital priority.

As we head to a turning point in IoT security, we anticipate that dependence on the RoT will grow exponentially as the ecosystem looks to establish trust at all stages along the value chain. Entities will seek to use the RoT and critical functions both in software and end-products or devices. Third-party security labs and independent testing will look for the RoT to verify trusted components. The desire to build IoT security and a RoT will be prevalent at every stage of the product design cycle.

> “Starting at the core, we talk about secure by design a lot and having trusted components within an organization or system allows us to compartmentalize where we’d see that risk. That keeps the cost of failure to a minimum.”

Munich RE | **Tim Davy**, Cyber Security Specialist, Munich Re

A Future Under Construction

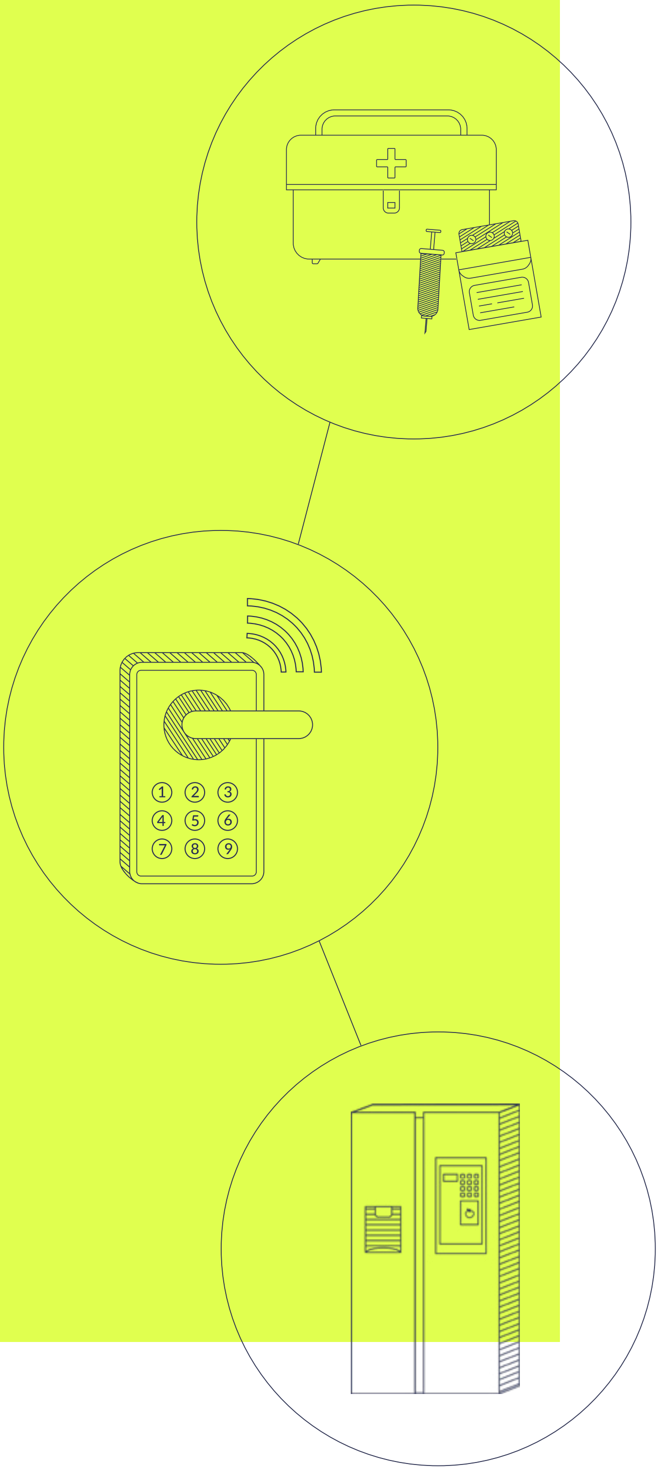
Consumer

Home Automation (Speakers, Thermostats, Appliances and Lighting), IoT For Good (Climate Change, Air Quality Monitoring, Vaccine Delivery), Healthcare Monitoring and Security (Smart Door Locks, Doorbells, Cameras and Alarms)

As with the cities we live in, the consumer mindset is set to rapidly change over the coming years, especially considering the digital-first decade into which we are heading. Home automation and healthcare are taking center stage and as our technology becomes increasingly capable, its impact on wellness and health monitoring will grow too.

In fact, a huge 78% of surveyed wellness and health monitoring respondents believe building on the RoT is most important for their companies – the largest of the groups surveyed. The consumer IoT survey respondents were also the group who most strongly believed that individual companies should be taking the initiative for protecting consumers from vulnerable cyber products (58%).

Amidst the continued uncertainty around working from home, there is a reliance on IoT technology, and it’s clear that the consumer market is mindful of the steps to be taken in order to protect consumers from vulnerabilities.



Barriers, Costs, and the Need for Action

Executive Summary

It’s clear from the report thus far that the world is reaching a technological turning point, becoming more connected, and as a result, ever more reliant on those connections. Both businesses and consumers are aware of the benefits of IoT and are quickly waking up to the fact that greater IoT security brings more benefits.

While it is true that there is growing readiness around IoT security, there are still barriers to be addressed, whether in terms of broader and more detailed education or the cost of development and implementation. Our findings show that although businesses are becoming more satisfied with their in-house security expertise, there is still room for improvement.

Despite insufficient resources internally, companies are not investing in external experts to conduct validation and testing. It questions whether security budgets are being spent on the right things.

None of these issues are insurmountable. They are merely obstacles to a brighter future. Our respondents agree that we need to be working closely together with collaboration and best practices to overcome challenges.

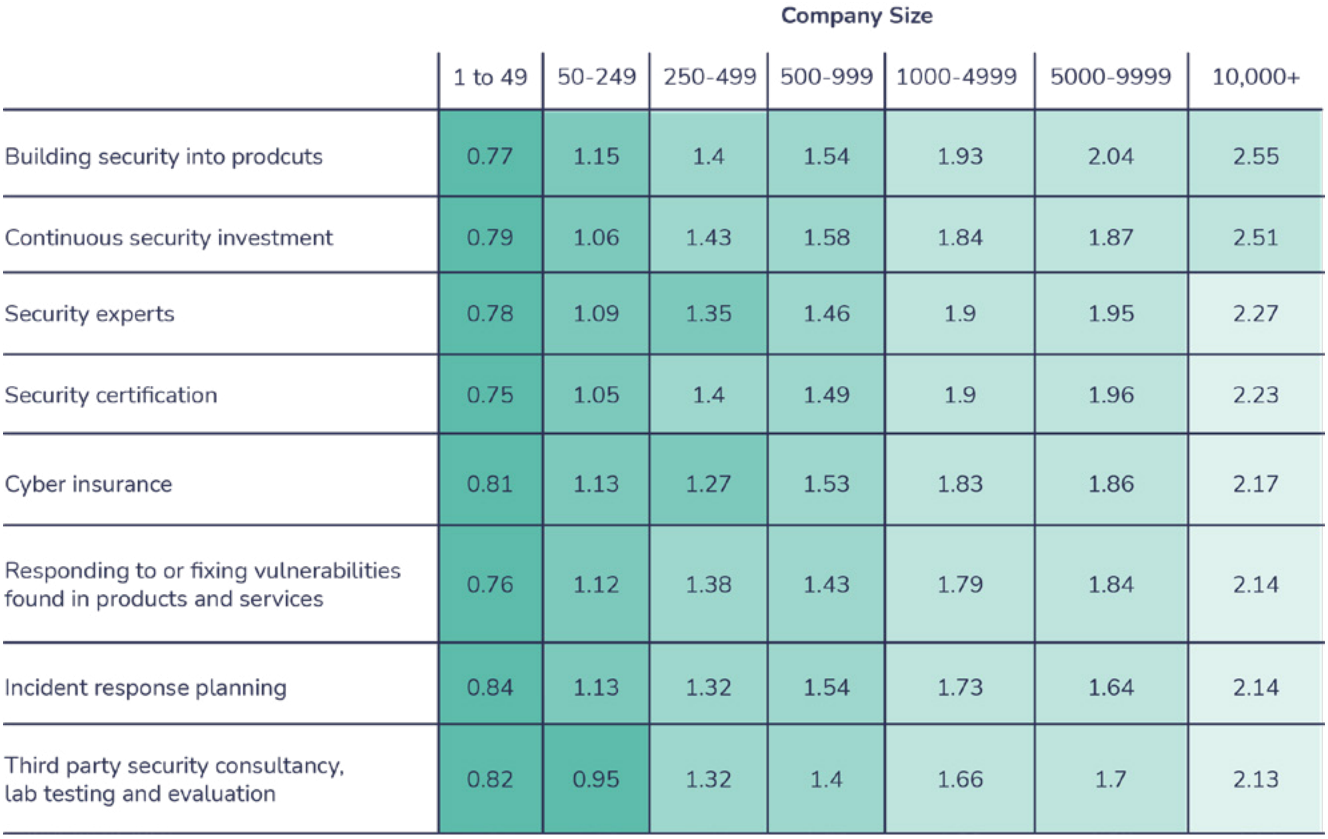
The IoT Security Cost Paradox

It's clear from the research that IoT security has been recognized as a critical priority for 2022 and is the foundation of change ahead. Our respondents say the most significant risk to the successful deployment of digital transformation is security concerns about product vulnerabilities. However, we can't deny that security will remain a problem without proper resourcing. One of the common recurring issues both in our previous and in this latest report is the notion of cost, both in terms of physical dollar costs and the cost of security experts and independent evaluation.

Security Budgets

The cost of securing the IoT is challenging for organizations of any size to forecast and accurately budget. In our survey, respondents estimate their companies spend an average of US$1.56 million a year on building security into products – the highest of any budget spend.

Average spend by company size (US$)



	Company Size						
	1 to 49	50-249	250-499	500-999	1000-4999	5000-9999	10,000+
Building security into prodcuts	0.77	1.15	1.4	1.54	1.93	2.04	2.55
Continuous security investment	0.79	1.06	1.43	1.58	1.84	1.87	2.51
Security experts	0.78	1.09	1.35	1.46	1.9	1.95	2.27
Security certification	0.75	1.05	1.4	1.49	1.9	1.96	2.23
Cyber insurance	0.81	1.13	1.27	1.53	1.83	1.86	2.17
Responding to or fixing vulnerabilities found in products and services	0.76	1.12	1.38	1.43	1.79	1.84	2.14
Incident response planning	0.84	1.13	1.32	1.54	1.73	1.64	2.14
Third party security consultancy, lab testing and evaluation	0.82	0.95	1.32	1.4	1.66	1.7	2.13

Q. How much do you estimate your company is spending on each of these areas every year in US dollars? Please select an answer: <US$500K, US$500K – 1M, US$1M-2M, US$2M-3M, US$3M-4M, US$>5M, I am unsure

As we can see from the above chart, respondents also invest US$1.53 million on average on continuous security processes. In contrast, respondents spent a further US$1.5 million on security experts and security certification, respectively. These were ranked marginally higher in terms of spending than cyber insurance (US$1.48m) and responding to or fixing security vulnerabilities (US$1.46m), signalling a gradual transition to a more proactive and preventative approach to security.

Of course, the amount spent on security scales with the size of the company – where companies of 1-49 employees spend US$0.77 million on building security into products, and companies of 10,000 spend US$2.55 million. This further underpins the findings of the PSA Certified 2021 Security Report, where the democratization of security for companies of all sizes was deemed essential.

We anticipate that the gradual transition will be accelerated in 2022, as best practice guidelines, a common language around security, and trusted components will help streamline costs and further level the security playing field.

Security Experts

Beyond direct dollar costs, other cost factors are at play that impacts the IoT ecosystem. According to our research, the main barrier to IoT security is a lack of security specialists (30%), followed by a lack of understanding of security expertise and complexity, both at 24%. The lack of security professionals is systemic to a population wider than our surveyed group - the World Economic Forum estimates a gap of over 3 million cyber security professions needed worldwide.

Although 94% of those surveyed are at least somewhat satisfied with their level of security expertise, only 31% of those people feel "very satisfied". There is some clear room for improvement here, especially when 59% say their engineering teams use internal validation to certify security implementations. Products built without sufficient security expertise and not independently tested leave space for vulnerabilities to be missed and exploited.

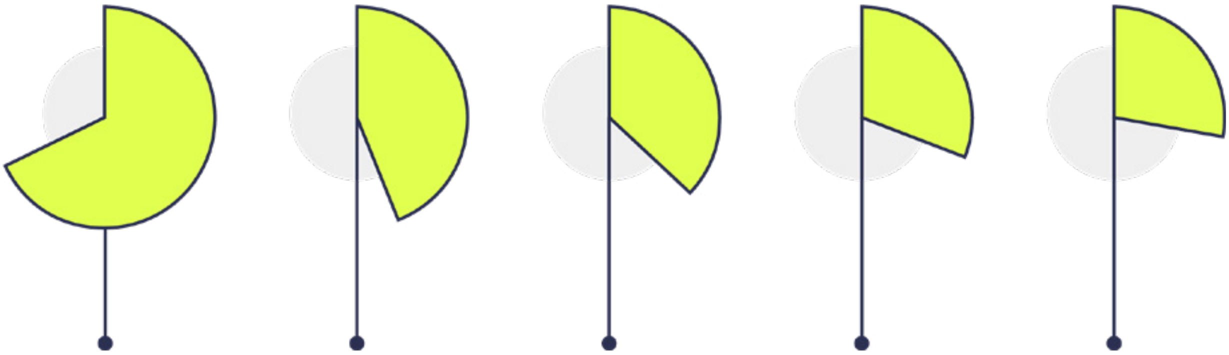
Optimizing Security Expertise

Our findings show that 95% of respondents do not currently conduct external lab testing as it's perceived to be too expensive. To maintain pace with the evolving desire for security, this does call into question: are budgets being allocated and assigned correctly? Especially when 4 in 5 respondents agree that security has increased as a priority over the past 18 months, with over a third saying they believe distributed working and the pandemic have increased the likelihood of IoT hacks.

> "At eInfochips, an Arrow Electronics company, we understand how the lack of security expertise can be a barrier to delivering secure solutions. Working with clients, we augment their skills with our edge-to-cloud security expertise. We help design, develop and manage secure connected products that leverage PSA Certified components, resulting in more robust solutions."

eInfochips An Arrow Company | **Bharath Aitha**, Vice President - Marketing, eInfochips

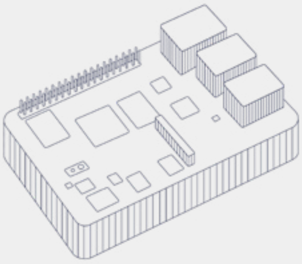
The most important options when considering creation of "secure devices" are:



68%	44%	37%	31%	28%
Building with trusted components / Building on a Root of Trust	Over-the-air updates	Third-party security certification of devices	Completing threat modeling before building devices	Buying insurance/ warranty products

Q. Select the three most important options when considering creation of "secure devices" and ultimately

Off-the-shelf Trusted Components



Components with a certified Root of Trust that, for example, contain all the keys used for cryptographic functions, performs secure boot, enables secure configuration and secure code execution are inherently trusted, because they have been developed through a secure-by-design approach, and ideally, independently certified.

There is a clear theme in our data that off-the-shelf trusted components (those that include a Root of Trust), are increasingly being demanded in the ecosystem. In fact, when asked what would make IoT security easier to deploy 46% of respondents asked for "off-the-shelf product solutions".

The PSA Certified ecosystem is providing exactly this, with over 20 silicon vendors that have adopted the PSA Root of Trust (PSA-RoT) which software providers and device manufacturers are building upon and reusing time and time again in designs. In fact, PSA Certified Original Design Manufacturer (ODM), Flex and solutions distributor, Arrow are providing full development platforms which will make security components easier to reuse than ever before.

They know that if we are to create an ecosystem that offers IoT security today and into the future, manufacturers will need to be able to choose trusted components that are assured of a Root of Trust at the silicon layer, forming the foundation on which all secure operations of a computing system depend.

> "We're not surprised to hear that nearly half of IoT decision makers are seeking off-the-shelf product solutions in order to help them deploy secure solutions and with the announcement of cyber security requirements to be part of the future RED CE certification procedure in Europe, this percentage will increase in the next years. Our customers tell us that our PSA Certified development prototype designs like iENBL, help them to fast-track new product designs into the market, without compromising on cost or security functionality. At Flex, we think this will be a trending topic in 2022 and we're proud to be part of the PSA Certified ecosystem delivering real-world solutions."

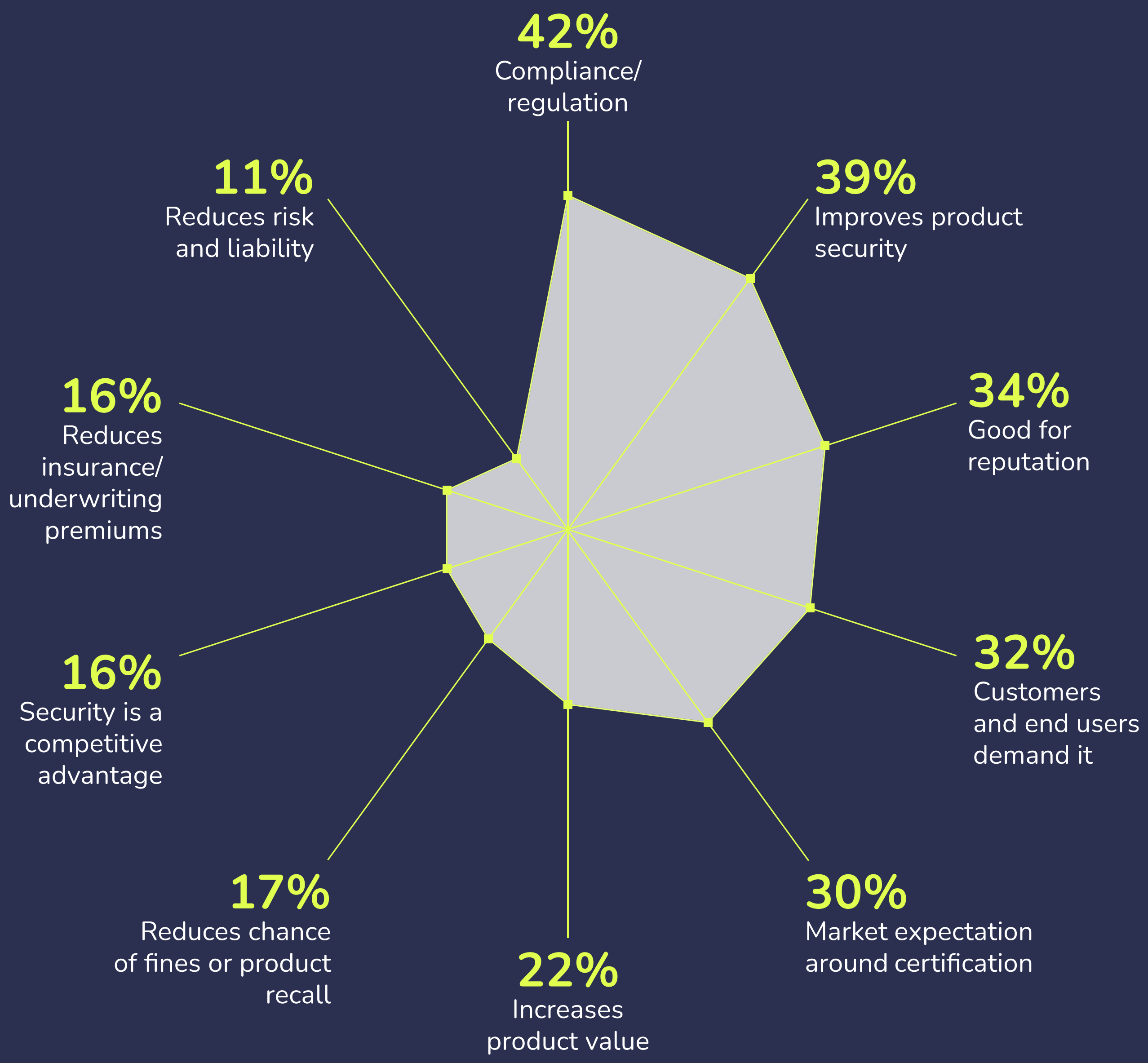
flex

Dr. Juan Nogueira-Nine, Sr. Director - Connectivity – Global Technology Team, Flex

There are multiple benefits to using third-party labs too. Unsurprisingly, 42% of decision makers say they seek certification because of compliance/ regulation. Regulation challenges emerged very strongly in our last report. We believe it is likely to increase further as regulation is rolled out in different territories, primarily as business compliance may become mandatory to sell in specific markets.

Other reasons to seek certification included 39% reporting that it is an excellent way to improve the security of products and 34% agreeing that it benefits company reputation. In other words, those that do work with external labs - and invest in IoT security certification - are experiencing the benefits of independently verified IoT security. In many cases, we are missing the opportunity to prioritize actively preventing security breaches upfront, instead of relying on damage limitation later.

The main drivers behind working towards security certification with security labs:



Q. What are the drivers behind working towards security certifications with security labs? (Select all that apply)

As we delve deeper, there are other spaces where, as an ecosystem, we could actively work to prevent security vulnerabilities. In the PSA Certified 2021 Security Report, we found that threat modeling, a critical step in identifying and mitigating breaches, was skipped by our respondents. The findings are almost identical in this report, with only 44% carrying out threat modeling on most new products. This is problematic, as ecosystem adoption of threat modeling is fundamental to enable security by design. It allows every product and supplier to build security into products from the ground up.

If we are to overcome the barriers to IoT security, we need to look at how we can equip businesses of all sizes with security knowledge and frameworks (such as those provided by PSA Certified) to deliver trust and benefit the whole industry.

Fortunately, we can see the start of this trend, and we're going to talk more about the solutions on the horizon in the next section.

> "The PSA Certified 2022 Security Report provides insights into the industry's market needs and provides guidelines to help build secure IoT devices. It also highlights the need for making threat analysis a standard exercise when launching IoT products. As well as the applicability of security capabilities for applications such as cyber insurance and IP protection. All this market intelligence will help us to make informed decisions and support IoT developers in 2022 and in the future."

SGS brightsight

Carlos Serratos, Senior Director Strategy, Policy and Advocacy at SGS Brightsight

A Future Under Construction

Smart Cities

Transportation, Building Automation, Commercial IoT, Asset Tracking and Smart Energy

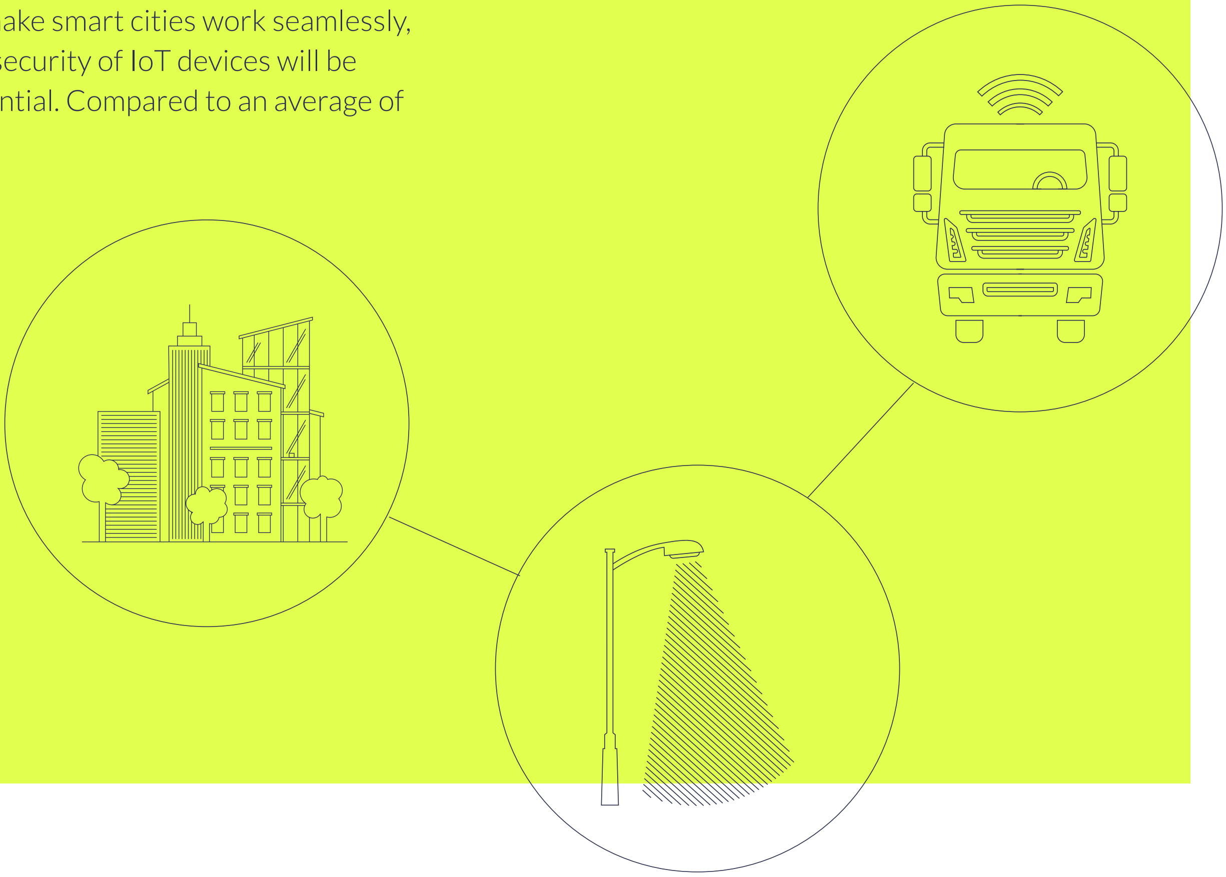
The IoT, becoming increasingly capable through technologies like 5G, is going to change cities as we know them. Cities, especially a metropolis like London, Tokyo, New York or Singapore, have traditionally been hotspots for innovation and early tech adoption, and that is going to accelerate in 2022.

In fact, everything about cities will change in the decade to come, from how they're run and built to how people live in them, to the point that they become 'smart cities'. McKinsey and Company define smart cities as those that "...put data and digital technology to work to make better decisions and improve the quality of life" - cities that are underpinned by smart integration between transport, energy, and retail & distribution.

To make smart cities work seamlessly, the security of IoT devices will be essential. Compared to an average of 37% across all respondents, 46% of smart city respondents state that security is a priority for their business because their customers demand it. This not only highlights how advanced end users are in terms of expectations, but also emphasizes how quickly IoT security is becoming a fundamental part of our cityscapes.

When it comes to designing IoT devices for smart cities, 84% of smart city respondents are most likely to think their company follows best practices when developing connected devices.

We are already seeing that for the IoT ecosystem to grow and meet the demands of smart cities it must adopt the same principles of mutual agreement collaboration and guidelines to flourish.



The Role of Collective Accountability

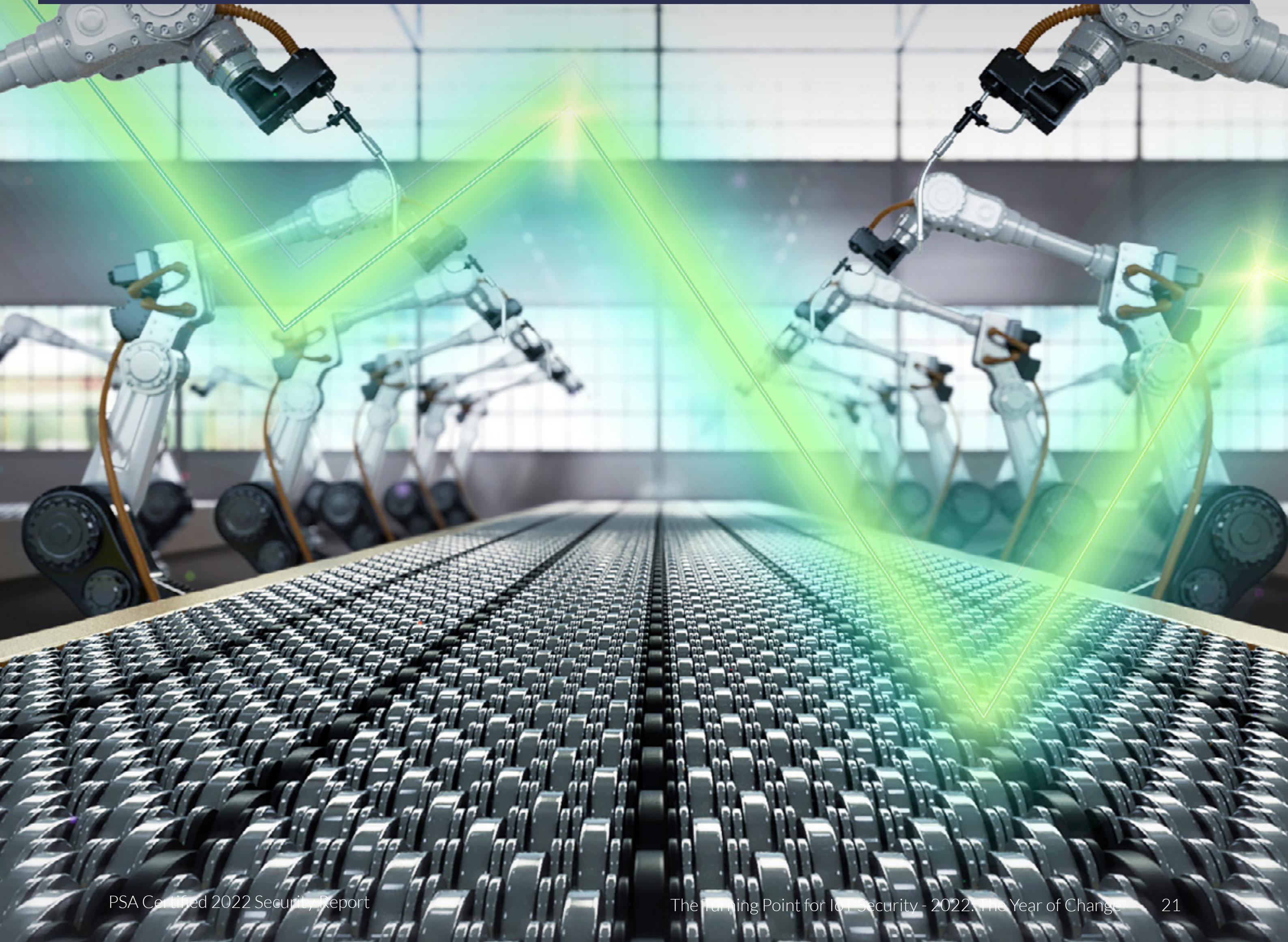
Executive Summary

If the IoT is going to fulfil potential, guidance and education on IoT security are crucial. There is agreement across the ecosystem, regardless of segment, company size or vertical, that we as an industry are all on the same path. By working together, we can build a more secure IoT faster.

When we think about the accountability of the IoT, we inherently think about governance and responsibility. Who is held accountable should issues arise at different points along the value chain? And how do those entities interact to mitigate hacks and keep user privacy intact?

Our research highlighted that it would require industry guidance and community collaboration, with 96% of respondents interested in an industry-led set of guidelines to help build IoT security. The willingness to collaborate is considerably higher than our inaugural report (84%).

These figures tell us two things: people are increasingly prepared for IoT security but need guidance from leaders on how to implement it. No company should now disagree that IoT security will be built around accountability, a common language and third-party certification.



Filling the Knowledge Gaps

Knowledge gaps are creating a disparity within the IoT. Those that are already implementing and showcasing security are seeing the benefits already. However, access to knowledge and security best practices could quickly change this. IoT security will soon become a standard, not a premium, if everyone has access to the same information and tools. So, what does the ecosystem require to fulfil the knowledge gaps? There are two key areas: third party certification and industry collaboration.

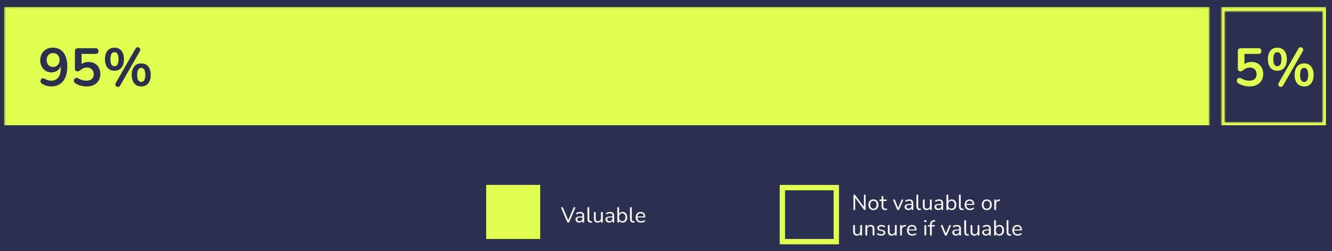
A Common Language and Third-party Certification

A key area to accountability is the ecosystem speaking a common language around what "best practice" means. Nearly 70% of those surveyed admit that, while they value seeing security credentials on products, they don't know which security credentials to look for when buying for their company. What's more, they admit they do not understand the questions they need to ask. One step to overcoming this hurdle is to use third-party certification and common frameworks across the industry so that we're all speaking the same language to define what "best practice security" means for IoT. Third-party certification provides a transparent security marker across the value chain, so when choosing trusted components (silicon and software) to build into a device, they can look for verified components. Our survey respondents agree - 95% believe that third-party security certification can be at least somewhat valuable to ensuring secure IoT.

Industry Guidance and Community Collaboration

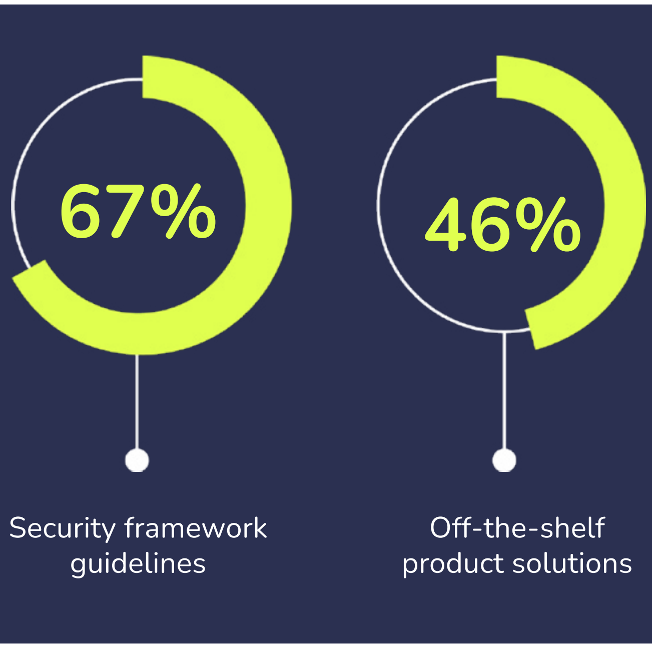
One thing that is very clear in the PSA Certified 2022 Security Report is that the IoT ecosystem is ready to collaborate and take guidance from security experts. 96% of those surveyed say they would be interested in an industry-led set of guidelines to help build IoT security. This has risen from 84% in our previous report, and we fully expect that this year collaboration will be a key part of security strategy. Building on this, 67% of respondents say they would value step-by-step guidance in helping deploy secure products.

Q. How valuable do you believe a third-party security certification can be to ensuring secure IoT?



If companies of all sizes are to be accountable and respond to the pressures and opportunities of IoT security, it is vital that not only time but also money needs to be invested. Companies need to leave space within their budgets to resolve current issues, and to develop future solutions. Not all these issues will be solved in-house, therefore looking to third-party processes and solutions will be vital for IoT success.

The top two requests from respondents when asked "What would be useful to you and your company to help you deploy secure products?"



The Role of Threat Modeling

Security begins with understanding not only how a device works as intended but also how it could be manipulated to work by those with malicious intentions. Analyzing the way it can be used, abused, accessed, and even altered is known as threat modeling.

A device should be designed, manufactured, tested, and certified based on the threat model used to architect and design the device, saving costs further down the development process and ensuring trust is built in from the ground up.

In our survey, we found that 44% carry out threat modeling on most new products, and 37% on every new product, while two thirds say security frameworks would be useful to help them deploy secure products (67%).

We maintain that a threat model is an imperative and must be created at the beginning of the product design to guide the architecture and design process of a product. This ensures that the right device security measures are mapped out before product development.

By incorporating threat modeling into the design process, you can determine how robust the security needs to be and what, exactly, you need to do to protect your IoT product.

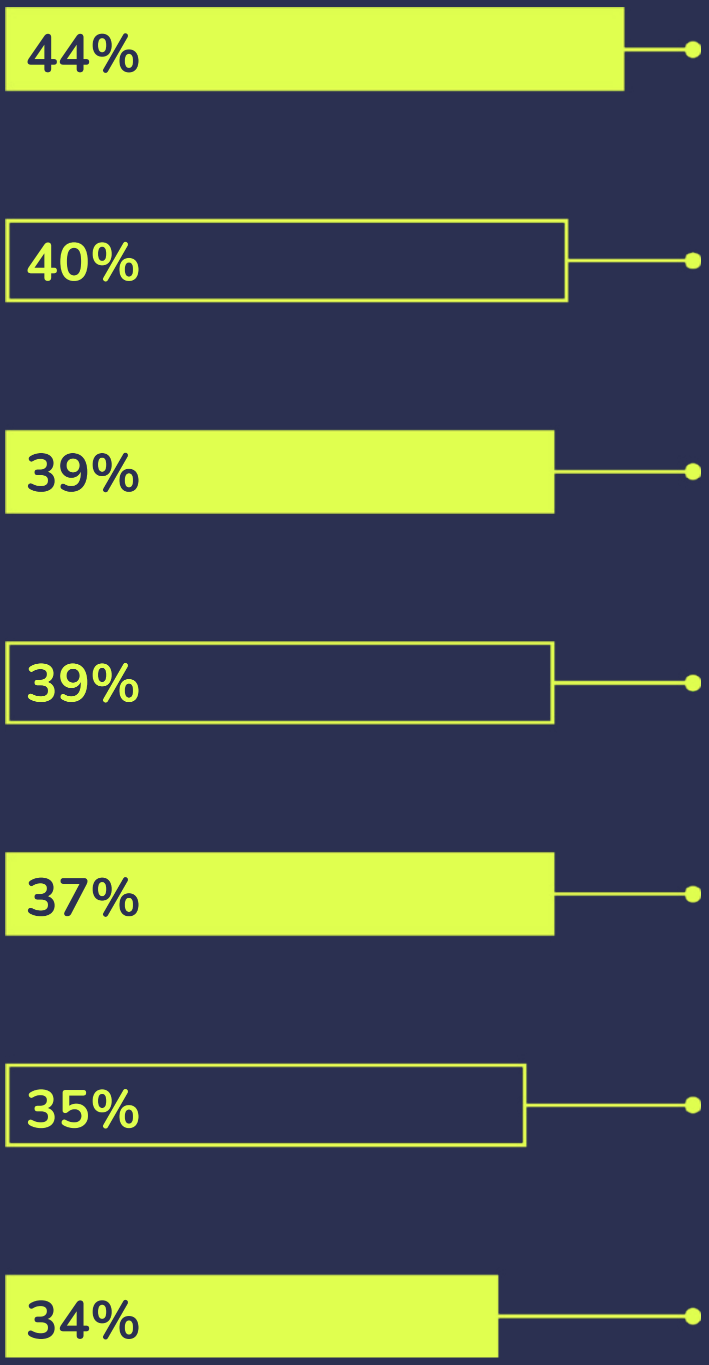
IoT Security Accountability

Continuing the notion of collaboration, it's clear from our research that the future of the IoT does not lie in the hands of one business or government, we all have a part to play. No single party was identified as holding the greatest responsibility, underlining the fact that collective accountability is key. To that end, through collaboration across the value chain and the use of certified trusted components, we can all take an active role in bringing the vision of the future IoT ecosystem to life.

"At Renesas, we have been designing and producing security-focused microcontrollers for over ten years, and we remain committed to investing in IoT cybersecurity technologies as part of our leading-edge 32-bit product development. We recognize that security is a collaborative effort and that we as a silicon manufacturer we must do our part to enable a secure IoT. For example, our RA Family takes advantage of Arm security architecture based on Armv8-M TrustZone technology, and we have implemented proven security technologies, including physical hardware security in our general-purpose microcontrollers that appeal to a broad range of connected applications segments. We also support independent certifications such as PSA Certified that assist IoT device developers to quickly identify products and solutions that offer cost-effective protection for IoT threat models."

RENESAS | **Daryl Khoo**, VP of Marketing, IoT Business Division, Renesas

Our research shows that everyone has a part to play in the future IoT ecosystem:



44% of respondents believe individual companies and businesses should be taking the initiative for protecting consumers from products introducing cybersecurity vulnerabilities

40% argue that it is the responsibility of governments

39% believe it is the duty of IoT product manufacturers

39% also believe that the task falls to industry associations and public sector making mandatory evidence of security for device procurement

37% say the responsibility goes to industrial and consumer associations creating or adopting labels, or product catalogs of secure products

35% say underwriting risk groups, making use of the evidence on the use of secure products for managing risk, providing cyber insurance policies with lower fees and/or additional coverage

34% believe consumers need to take individual accountability and appropriate actions.

Q. Who should be taking the initiative for protecting consumers from products introducing cyber security vulnerabilities? Select all that apply

Based on the above, securing the IoT is very much a collective effort, but bearing the brunt of the responsibility for IoT security will fall to businesses and companies. Everything depends on our willingness to adopt IoT security and the speed at which we do it together.

A Future Under Construction

Industrial

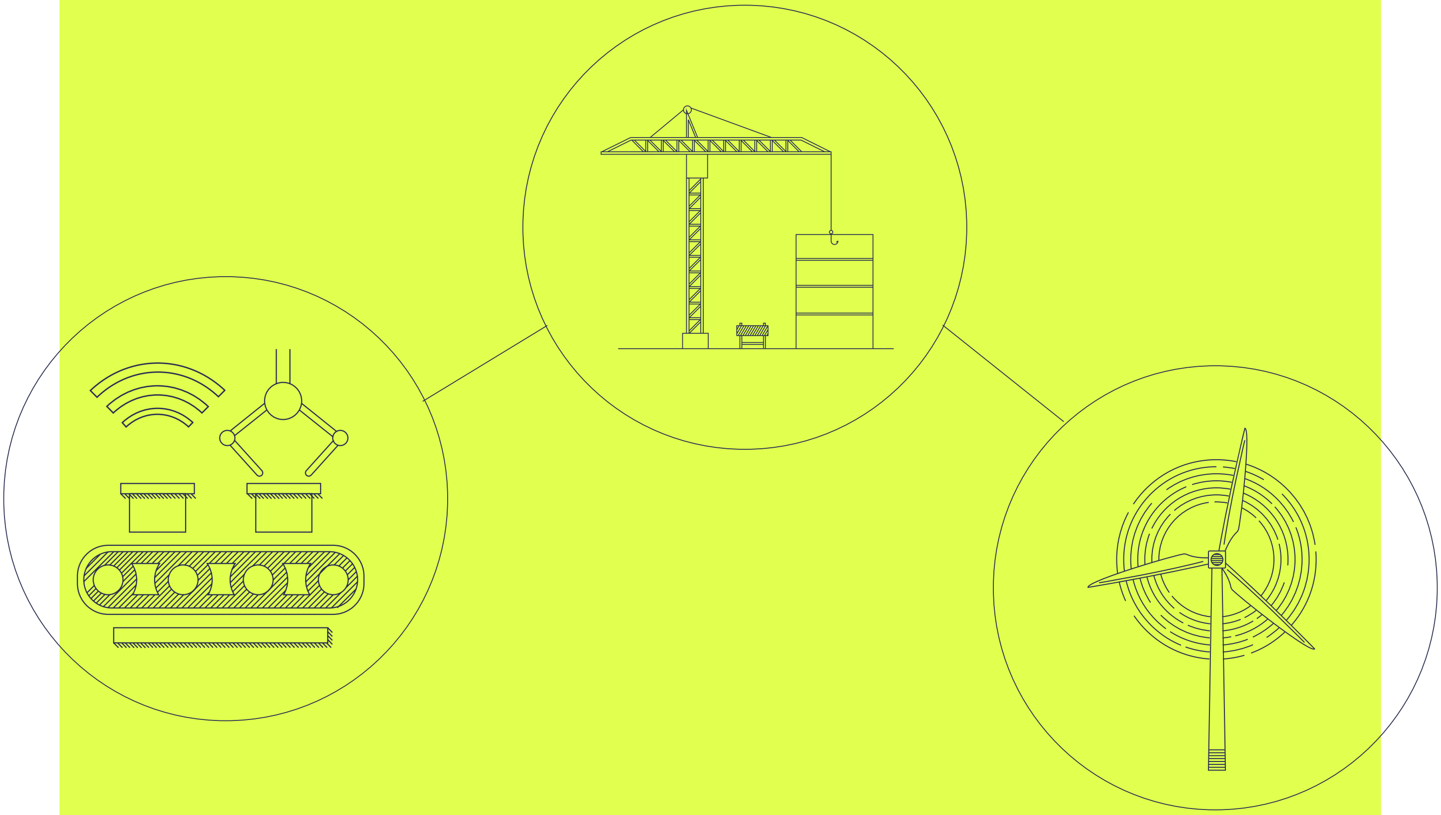
Industrial Machinery and Sensors, Smart Manufacturing, Smart Construction, Smart Supply Chain and Logistics, Big Energy and Smart Agriculture

The demand for housing, buildings, factories, and construction will never go out of style. It may redefine itself - new materials, new construction methods, greener buildings, sustainable assembly lines - but demand will forever be a constant, especially as the world population soars.

This demand was evident within our survey, as those within industrial sectors (including transport and construction) are most likely to spend US$5 million+ on continuous security investment, which is considerably above the average of US$1.3 million spent across all those surveyed.

It's clear that in many areas the industrial sector is striving to be ahead of the curve, in our survey they were the most likely (59%) to have implemented IoT into their systems, and 57% believing that having security in products positively impacts the bottom line because it allows them to sell to people and organizations that mandate a certain level of security.

Increasingly, these core parts of our society will come to rely on the IoT in more ways than one, from virtual construction sites to training and demos, therefore ensuring that best IoT security practice is essential if we are to see expansion continue at pace.



Conclusion

As the IoT continues to grow beyond early adopters, everyone from individual end users to global businesses will become digital to the point where the IoT underpins every function of our daily lives, helping to realize the digital-first decade.

The outlook for the future is bright. In this report, we've uncovered key indications that IoT security readiness is already here, and that people are waking up to the benefits of IoT security. Companies and their employees are asking for it, as are their consumers. However, while awareness around security is gathering pace, there is still a great deal to be done around education and delivering best practice. Only through collaboration and a common framework will we achieve a vibrant IoT ecosystem.

Since the IoT will influence everything we all do, we need to join forces to provide the guidance, support and knowledge needed to prepare ourselves for the digital-first decade ahead. This will begin with a common way of communicating about IoT security and using third-party certification will be key to this.

Digital transformation continues to accelerate, and there is officially now no turning back. If 2022 is to be defined by the steps we take to secure the IoT, then it must begin with the use of trusted components. By safeguarding every step along the value chain, we will not only secure devices, but also secure the future of our industry.

However, it is crucial we don't rely solely on trailblazers to make this happen. The IoT is part of our lives now and by 2030 will likely underpin them. The IoT, and its security, is therefore a global concern and it is only through global, collective action that we can fulfil our dreams for the future

How You Can Get Involved

With everything said thus far, what is the best approach to solving the key challenges? For PSA Certified, it boils down to democratizing IoT security, making it accessible, working with partners and stakeholders and continuing to bring IoT security to the forefront of all discourse.

We agree with those surveyed about the role of trusted components, and for all connected devices to have demonstrable security built on common, best practice principles. This enables silicon providers, software providers and device manufacturers to demonstrate and showcase their security credentials and add genuine value to the supply chain. The requirements of the scheme are tested independently, offering an unbiased assessment of security implementations.

Above all else, it tackles some of the key challenges we've listed in the report:

- A common framework, developed by experts, reducing the investment needed in security. This collaborative workflow can free up financial resources that can then be moved into other areas of a product, service, or business's digital transformation. This is especially important for smaller businesses with fewer resources to hand
- The framework includes threat modeling examples, free of charge to bridge the knowledge gap
- The certification program maps to government standards and legislation to help over fragmentation challenges

- Combined, this security best practice provides a path to certification that answers the needs of the whole value chain including original equipment manufacturers (OEMs), purchasers, and consumers by solving issues around fragmentation through collaboration. Plus, it offers testing of chips, software, and devices to ensure that we have a measure of good practice and that we're not releasing products into the market with known vulnerabilities.

96%

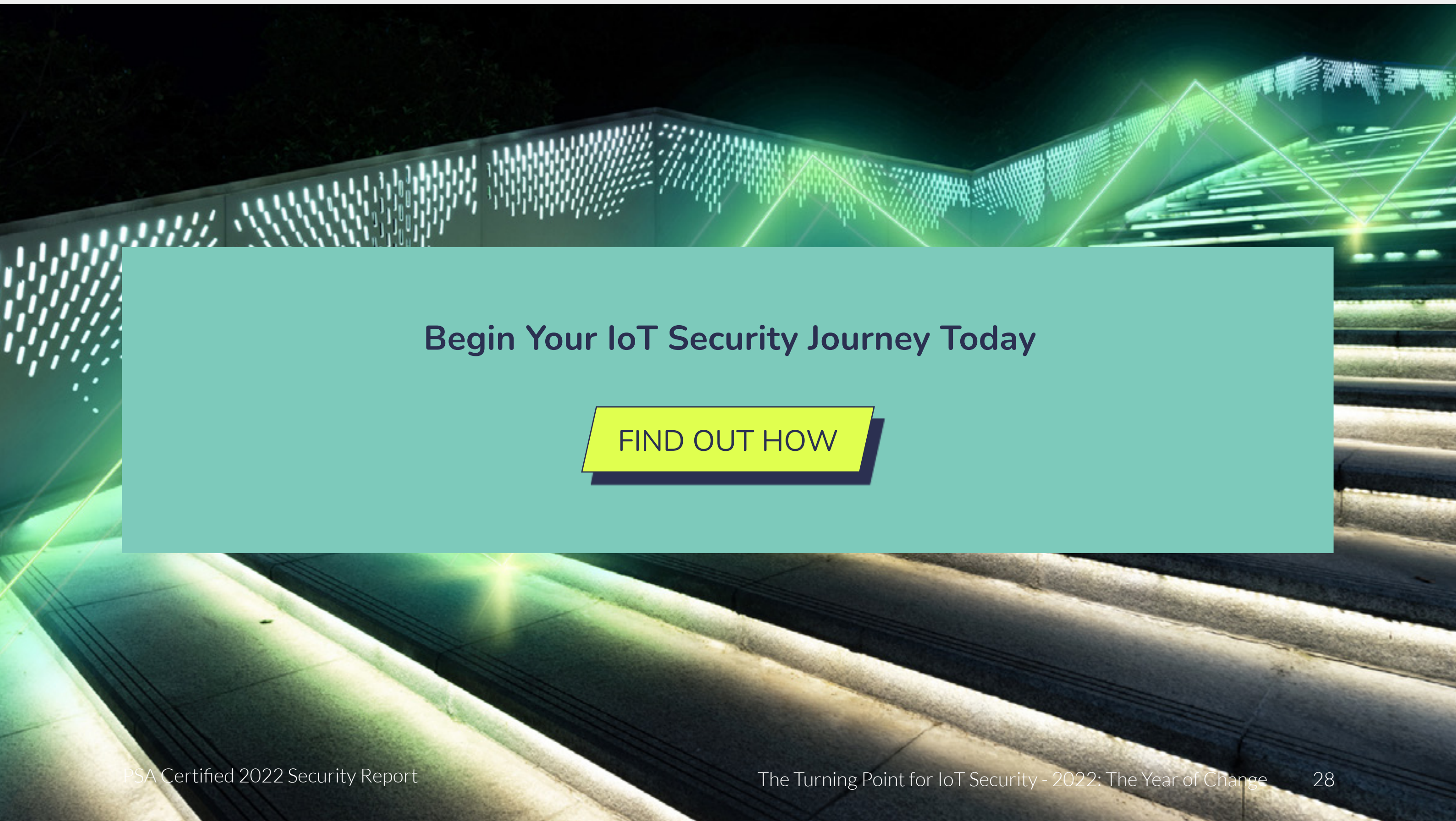
96% of respondents say they believe PSA Certified can bring value their company

92%

92% of respondents say they believe PSA Certified can bring value to IoT end users

To date, PSA Certified evaluation labs have evaluated nearly 100 products, from almost 50 partners. All our partners and our ecosystem are taking proactive steps in their design choices and working with external labs to demonstrate their security robustness.

PSA Certified is not something you achieve by luck; our partnership is leading the charge to make secure digital transformation a reality. Don't get left behind, join the fastest growing security ecosystem today - find out how.



Begin Your IoT Security Journey Today

FIND OUT HOW

Methodology

The core of the findings in this report were conducted among 1,038 technology decision makers and consultants in the US, Europe (UK, France, Germany, Italy, Sweden, Denmark, and Norway) and APAC (China, Taiwan, Korea, Japan).

Most interviews (1,014) were conducted by Sapio Research in November 2021 using an email invitation and online survey. The remaining interviews (24) were reached out to by Arm over email and social media.

Country of Residence

United States: **218**

Europe: **510**

APAC: **310**

Audience:

Silicon providers, software providers and device manufacturers: **51%**

Ecosystem: **49%**

Role Type

23% of respondents held C-suite/Executive level positions

37% of respondents held Director/Vice President level positions

41% of respondents held Manager level positions

Size of Company

1 to 249 of employees: **29%** of respondents

250 to 999 of employees: **33%** of respondents

1,000 to 9,999 of employees: **31%** of respondents

10,000+ of employees: **7%** of respondents

Company Type

Software providers: **32%**

Silicon vendors: **13%**

Original Equipment Manufacturers (OEMs) and Original Design Manufacturers (ODMs): **6%**

Cyber insurers: **3%**

Other types of companies in the IoT ecosystem: **46%**

Vertical

43% of respondents were in an organization that served the smart cities industry

35% of respondents were in an organization that served the consumer IoT industry

27% of respondents were in an organization that served the industrial industry

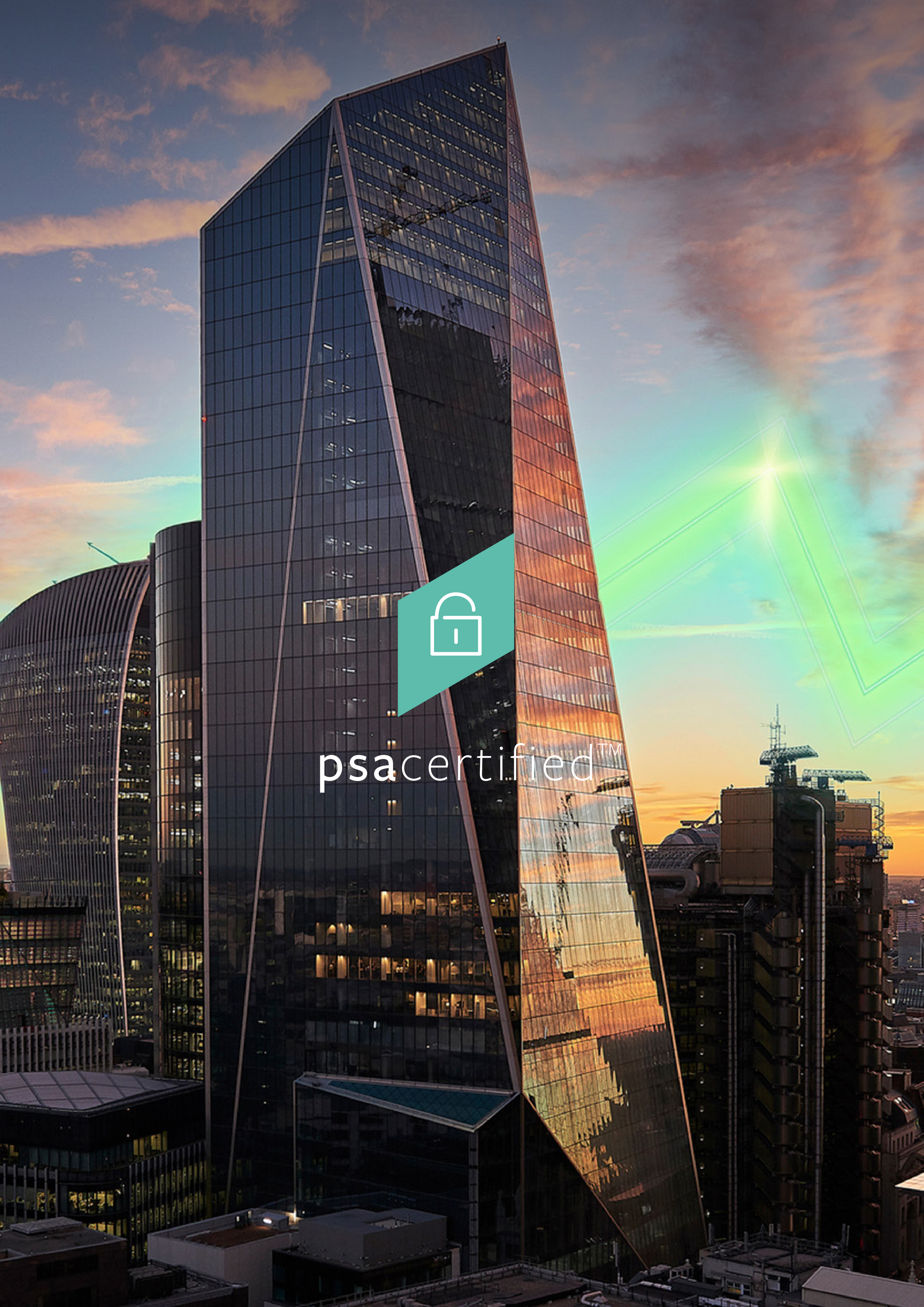
27% of respondents were in an organization that served other industries

Note: the above doesn't not add up to 100% due to respondents in some cases serving multiple sectors

At an overall level, results are accurate to ± 3.0% at 95% confidence limits assuming a result of 50%.

Where additional sources and data points have been consulted, citation is provided in the report.

While every effort has been taken to verify the accuracy of this information, Arm cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report.



psacertified™