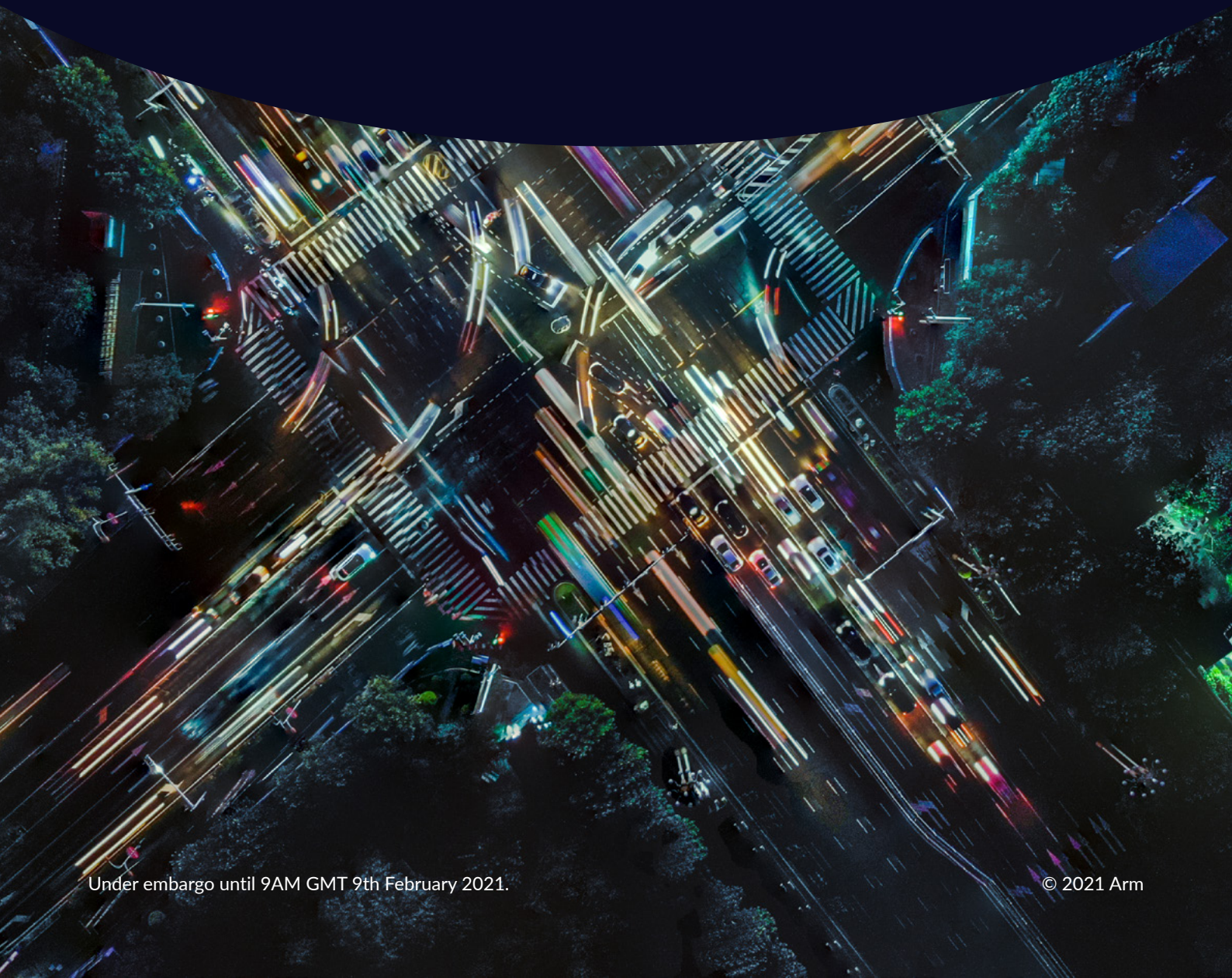
psacertified™

PSA Certified Security Report 2021

Bridging the Gap



Under embargo until 9AM GMT 9th February 2021.

Contents

1. About PSA Certified

2. Introduction

3. Summary of Findings

4. The Threats Facing the IoT

- Summary
- The Numbers Behind the Hacks
- A Growing Awareness
- Problem Areas

5. Value Chain Challenges

- Summary
- Barriers to Security Implementation
- Threat Modeling Adoption
- Where Does Security Responsibility Lie?

6. Bridging the Gap

- Summary
- The Role of Certification
- A Collaborative Future
- Redefining IoT Security

7. Conclusion

8. Methodology

About PSA Certified

PSA Certified offers a framework for securing connected devices, from analysis through to certification. The framework provides standardized resources to help resolve the growing fragmentation of IoT requirements and ensure security is no longer a barrier to product development.

PSA Certified accelerates device makers, system software developers and chip vendors through the process of achieving IoT s**ecurity ce**rtification through four stages: Analyze, Architect, Implement and Certify.

Built by experts and maintained by seven founding companies (Arm, Brightsight, CAICT, Prove & Run, Riscure, TrustCB and UL), PSA Certified represents an independent collaborative effort that's flexible enough to change with industry and geographic demands.

The scheme has seen significant momentum since launch in 2019, now featuring 55 PSA Certified products from 30 partners: Arm, EcoLux, Embedded Planet, Express Logic, Flex, Foundaries.IO, FreeRTOS, GigaDevice, Haier, Infineon, Ingeek, Lierda, Linaro, Microchip, Nordic, Nuvoton, NXM Labs, NXP Semiconductors, Renesas, Security Platform Inc, Qinglianyun, RT Thread, SDT Inc, Silicon Labs, ST Microelectronics, UNISOC, Veridify, Winbond and Zaya.

Find out more: psacertified.org/

Introduction

The rapid ascendency and popularity of the Internet of Things (IoT) has facilitated incredible opportunities for the digital transformation of goods and services. However, as the number of global connections scales and we see the world embracing digital transformation across multiple sectors, we also see a rise in cyber security threats. Hackers now have a myriad of new markets and verticals to focus on and exploit. This brings manufacturers and vendors a new set of risks that can not only affect their reputation, but also their bank balance.

As we embrace this new world, we'll start to recognize that device-level security is critical, and businesses will start to mandate good practices in their supply chains. It will touch every area of the ecosystem, from chip to cloud. We'll also see other influencers taking charge: including governments exploring legislation and cyber insurers who will want to quantify risks.

Security implementation doesn't come without barriers of course. Some of the most prominent IoT security challenges center around manufacturers and software vendors working in fragmented siloes, whilst weighing up the cost of security implementation against wanting to keep the cost per unit as low as possible. These tensions are met with further challenges: such as the lack of resources and security expertise, especially in smaller companies.

On one hand, we have an industry that knows we need to tackle security to succeed, and on the other, we're seeing devices in market without a baseline of security, lacking best practice implementation – paired with growing hacks, fragmentation of standards and a fast uptick in device shipments. This leaves a glaring gap between where we are now and where we need to be. These are the challenges we need to solve and bridge, but also opportunities in the making.

At PSA Certified, we're passionate about providing sought-after collaboration across the value chain. We know that following common cybersecurity requirements together can provide a route forward to our destination: healing endemic fragmentation and improving the security of connected devices. It is only together as an industry that we can address the causes of security breaches; in doing so we can arrive at a more powerfully and vibrantly connected future.

It was imperative to commission this inaugural PSA Certified Security Report. We needed an up to date comprehensive study into the attitudes, the practices, the pitfalls and the possibilities that the IoT brings about. We studied the opinions of 600+ decision makers in IoT to truly understand the problems they are facing, and what challenges still lie ahead.

Drawing from survey answers, a variety of external data points and our own industry insight, we have mapped the landscape of the connected device industry – and in doing so learned why the future of digital security will come as the direct result of unprecedented technological collaboration.

We hope you enjoy reading our findings. Collectively we can allow the true potential of digital transformation to be realized over the next decade, at a scale we have not yet even started to fully comprehend.

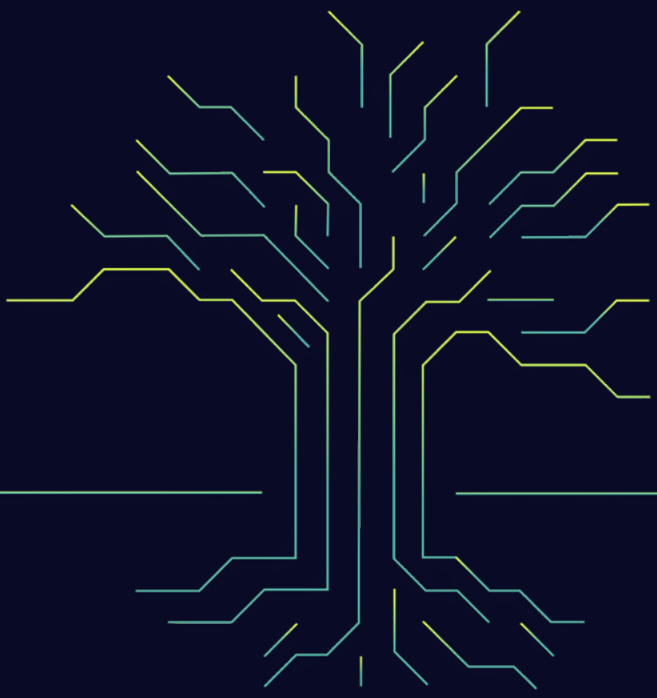
David Maidment

Director
Secure Device Ecosystem
Architecture and Technology
Group Arm

Bridging the Gap: Key Findings

61%

In our survey, we identified a gap between the perceptions of security implementation where 61% say we're on track with security – and the reality – where we're skipping threat modeling, lacking resources, struggling with fragmentation and not using third-party labs to validate security robustness. While we battle these challenges, devices are continuing to ship, and the number of cyber-attacks is rising.



The appetite for security is growing: the majority of respondents cited a need for security to provide differentiation for their product against competitors. We're also seeing growing awareness of Root of Trust as a baseline for security.

47%

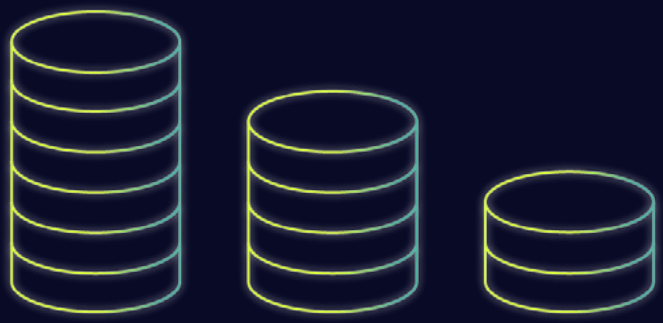
Staggeringly under half (47%) – said that they carry out a threat analysis in the design of every new product. Presenting a significant issue with best practice security processes being skipped, this is glaringly more problematic in smaller companies where the threat analysis of new products drops to 33%.

48%

Differing standards and regulations are seen as a top challenge by 48% of respondents, while 42% cite a lack of understanding or expertise within their business. Again, smaller companies are struggling (with only 33% satisfied with security expertise in their company) which suggests security needs to be democratized so that all companies – no matter their size – can implement security solutions.

54%

Cost of security is still a blocker: "Uncertain on ROI" and "lack of buy-in" account for a combined total of 54% of respondents who cited an unwillingness to invest continuously in security measures.



84%

of tech decision makers show interest in the development of an industry-led set of guidelines and processes to help build IoT security.

Ultimately, these issues point to one conclusion: that fostering a connected-devices industry that embraces collaboration in the security space – of the kind made possible by PSA Certified – will reduce costs, reduce doubling up on work, and therefore free up previously misspent resource for other, pioneering areas of a company's digital transformation.

The core of this report's findings originate from a November 2020 survey conducted among 628 technology decision makers across Europe, USA and APAC by Sapio Research.

The Threats Facing the IoT

Summary

The view on security readiness from the technology industry shows an industry on the brink of transformation, but one wary of the dangers presented by hacks that continue to target new, emerging device markets. At every step along the value chain, we see anticipation of huge changes in IoT over the next few years (even those in traditionally slower-moving sectors). However, we also see varying levels of confidence in security measurement rollout and capabilities – as well as an industry slightly out of step with its own perceptions.

Adding to this is a disparity between the security capabilities of small companies compared to larger ones, and a growing disconnect between security knowledge and security implementations. As deployments scale, we can only expect pressures to increase.

The Numbers Behind the Hacks

Security is never a solved problem – it's an ongoing journey. That's especially true in a world where products, companies and whole industries are embarking on a process of ongoing **digital transformation**. Security should be the bedrock of that transformative process; implementing strong security measures means technical assurance that a product or service can be scaled with confidence, and that it can deliver value. Without adequate security, you're building your business on shaky foundations.

As security analyst and journalist Brian Krebs puts it, "if what you put on the Internet has value, someone will invest time and effort to steal it."

The numbers supporting that statement ring true, and it's true for a whole new sector of devices. The **Cybersecurity Ventures Official Annual Cybercrime Report** predicts that by 2021 there will already be $6 trillion of cybercrime damage. **Symantec**, similarly, detected almost 19 million attacks on its honeypot IoT devices in the first quarter of 2020 – a 13% rise when compared with the previous year. In fact, **Symantec** – in its Internet Security Threat Report 2019 – estimates an average of 5,400 attacks on IoT devices every month.

5,400 attacks

So why, if that's so inherently true, are attacks still happening? And why are products still shipping with vulnerabilities? To find out why we are in this position, let's look at the trends and complications facing global security readiness.

> "If what you put on the Internet has value, someone will invest time and effort to steal it."
>
> **Brian Krebs, Security analyst and journalist**

A Growing Awareness

One of the biggest findings of our survey – and perhaps the most worrying – is the difference between the respondent's perception of security and the reality we're facing. Let's start with the fact that 60% of those questioned believe that their organization is 'ahead' with its IoT security implementation, while over three quarters (77%) of respondents are 'quite' or 'very' satisfied with the level of security expertise within their company. These are quite worrying statistics when you consider the stats, we discussed in the previous section looking at the growing number of hacks and devices shipping into the market.

The Gap Between Perceptions and the Reality of Security Implementations is Clear

Perceptions

61% Base: 628

3 in 5 tech decision makers believe organizations are ahead with their IoT security. Another 27% believe they are on track

87% Base: 434

are satisfied with the quality of IoT security implementations within their company

Reality

47% Base: 434

less than half of the same group carry out a threat analysis in the design of every new product

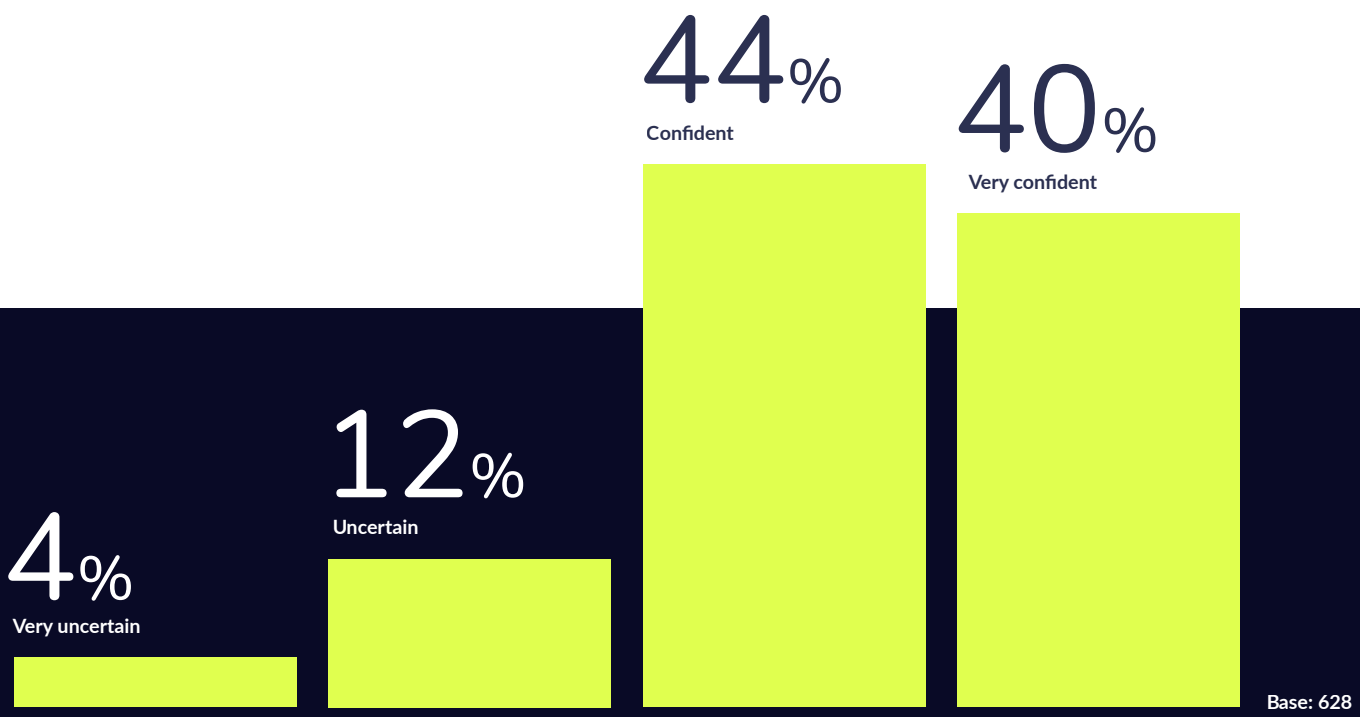
84%

84% of companies that have adopted IoT have reported some kind of security breach [Source: HPE]

Fundamental security best practices are being missed, in the meantime hacks are rising

Despite the disparity between perception and reality, we do see some trends in the right direction. Firstly, nine out of ten say IoT growth is critical to their business, and this appetite tends to bring with it a degree of positivity around security. Decision makers in the Transport and Logistics sectors are the most optimistic among this group, with most respondents (95%) believing an improvement in security standards will occur in the next five years. Secondly, we have a growing understanding of the term Root of Trust (RoT), where 84% would feel confident to define "Root of Trust" if someone asked.

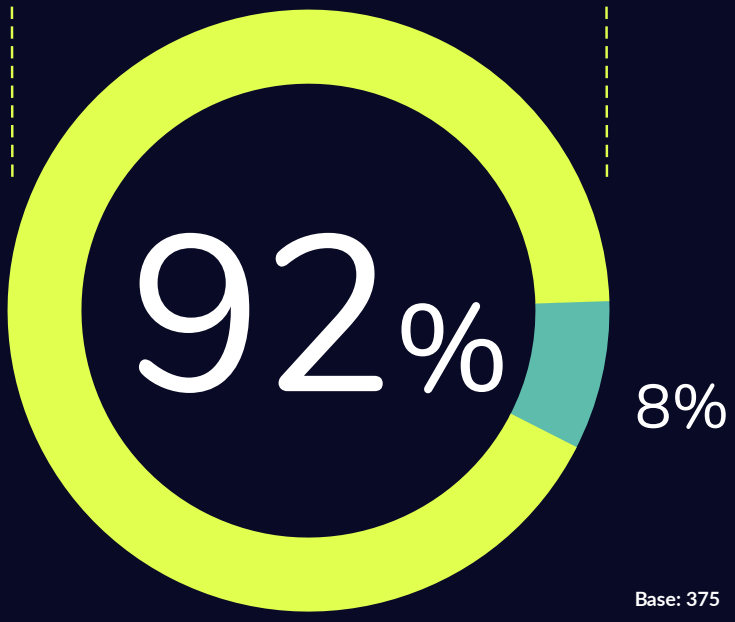
How confident would you be to define “Root of Trust?”



Are you deploying Root of Trust in your products?

92% Yes:
we include provisions for the Root of Trust in our products

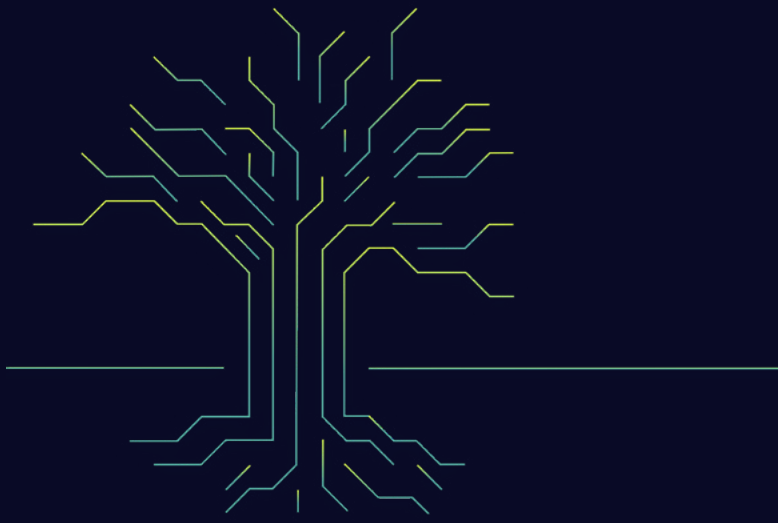
8% No:
we’re not including the Root of Trust in our products currently



What is the “Root of Trust”?

A **Root of Trust (RoT)** is the part of a processor where all the secure operations are performed, it has hardware protection and is separate to the non-secure processing environment which can be accessed more widely. Examples of secure operations in the RoT could include secure key storage, cryptography and attestation.

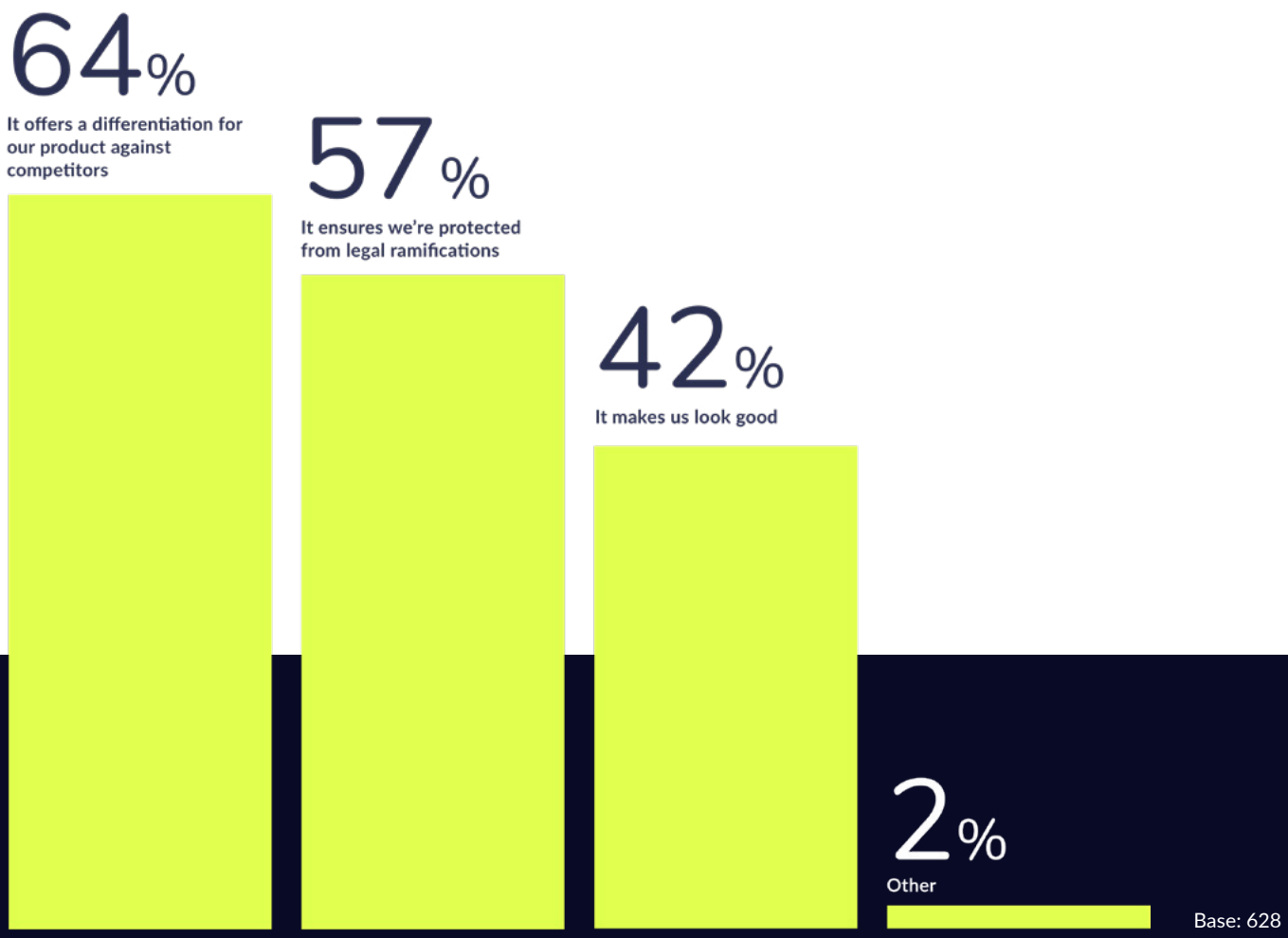
A RoT is crucial to ensuring a device’s integrity and crucial to ensuring the integrity and security state of that device can be determined by any other device or service it connects to.



We believe that part of this growing awareness is due to the mega trend of digital transformation – the mass acceleration of connected digital devices that deliver new business models, efficiencies and insights. Security is a key challenge to overcome for digital transformation to be successful and we're seeing positive signs that this is being recognized by the ecosystem. From our survey, the majority (67% - almost two thirds) of those who agree that security is important, do so because they believe it offers differentiation for their product against competitors.

We see this as a positive trend – security is slowly becoming a foundational benchmark that manufacturers need to meet. Although it's more often a hygiene factor over a headline feature, it can offer added value. Despite some of these positive trends, there are some problem areas which we'll discuss next.

Why is security important to you and your business?



90% Base: 628

of tech decision makers believe security to be important to their company, plus 90% agree security will be important to their company in 5 years time

93% Base: 628

believe that it's likely that security can be a differentiator in the IoT marketplace

Problem Areas

This all appears to be painting a promising picture, but there are discrepancies in the data that suggest the industry might believe it's further ahead than it actually is.

For one thing, satisfaction with security expertise isn't a flat landscape: instead, it scales with the size of a company. In our survey, smaller companies sized between 1-49 employees cited a 41% satisfaction rating, while larger companies of 10,000+ rank at 88%. So, it's clear that we need to ensure that we're democratizing security properly: good practice cannot be something reserved for the big organizations, it needs to be accessible to all companies irrelevant of their size.

Knowledge around Root of Trust, meanwhile, doesn't always match up to its deployment. While respondents in the US were amongst the most confident of respondents to be able to define 'Root of Trust' (87%), they were the least likely to be including provisions for it in their products. Respondents' ability to confidently define Root of Trust by itself varies in different countries too, with respondents feeling the most confidence in the USA and China, and the least confident in the UK, Taiwan and Korea.

Put simply: awareness of security requirements doesn't always match implementation and deployment.

The Size of Company Dramatically Impacts Security Implementation

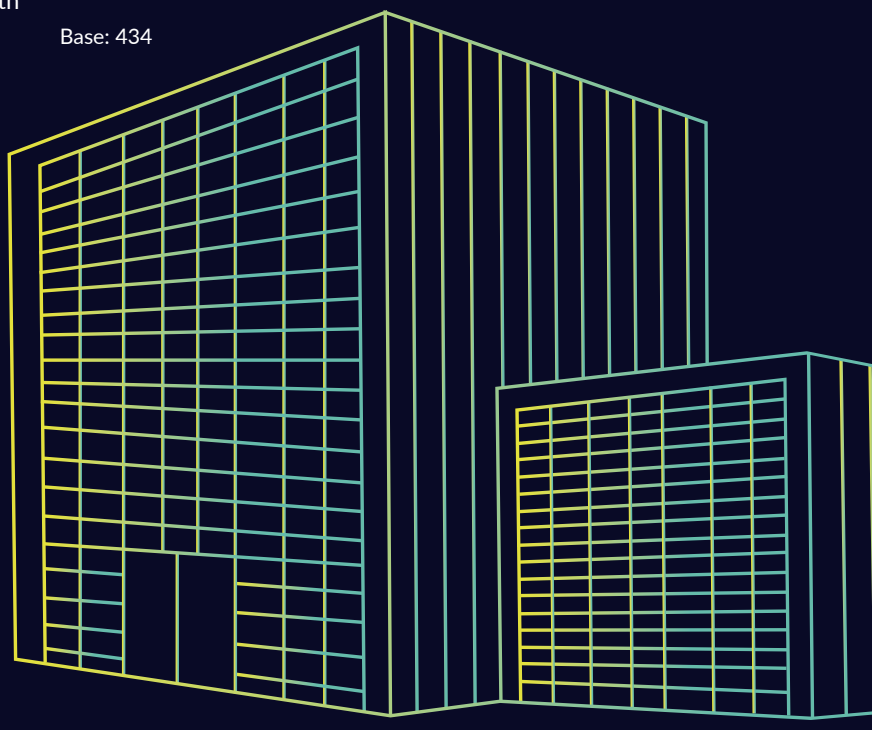
77% Over three quarters are satisfied with the level of security expertise within their company

41% are satisfied with the level of security expertise within their company sized between 1 and 49 employees

88% are satisfied with the level of security expertise within their company with over 10,000 employees

Base: 434

We need to democratize security so that any company, of any size can have a security solution



Value Chain Challenges

Summary

In this section, we explore the two core barriers to stronger security implementation: cost, and fragmentation – both of which impact threat mapping as well as the stage of a product's lifecycle at which security is properly considered.

Security is not a traditional feature that can attract a higher product price, which makes the business justification for stronger security implementation tricky. We have to remember; this is an industry that thrives when the cost-per-unit is as low as possible.

The true cost of security failure is hard for businesses to determine and budget for upfront, which makes determining the ROI of security a near-impossible feat. This is paired with an interesting debate around

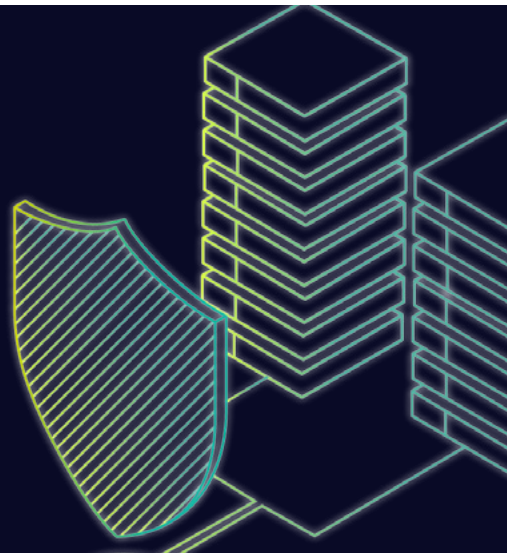
Barriers to Security Implementation

We've now established that the threats to IoT are growing despite a general trend towards security readiness – and that OEM security abilities aren't always in step with their perceptions – so there still seem to be barriers in the way of deploying products that inherit a security baseline to protect from the most common hacks.

To learn more, we surveyed OEMs to understand what is holding them back, with questions in three key areas:

- **The perceived pressing issues when it comes to security**
- **The barriers to investing in security**
- **Current challenges and barriers to implementing stronger security**

Across all three areas, we see two clear trends emerge: cost and fragmentation.



Let's tackle cost first. An OEM's need to create a device and sell it for a profit means it makes sense for them to closely manage the cost per unit associated with a device – both in terms of Research & Development (R&D), but also the bill of materials. Every moment spent creating devices comes at a cost, and that includes security. The challenge, however, is that security hasn't traditionally been seen as a feature that can innately command a price worth the extra investment.

This is evidenced by our survey results, which paint a vivid picture: half of the respondents consider the additional cost to be their biggest barrier to security implementation, with 42% citing upfront costs and R&D around security as the principal issues to overcome. That's over and above several other factors, including any damage to reputation or financial loss resulting from a security failure.

Although we're recognizing the need for security and the catastrophic effects if it's missing: many are struggling to justify the costs, or in some cases find the capital to resource the investment. When you consider the risks of skipping security, this does not paint a pretty picture. This is a key issue we need to overcome, and we need to democratize security in any way we can – ensuring that best practice security isn't reserved for those with the capital to invest.

Democratizing Security Is Critical for the Success of IoT

52% Base: 434

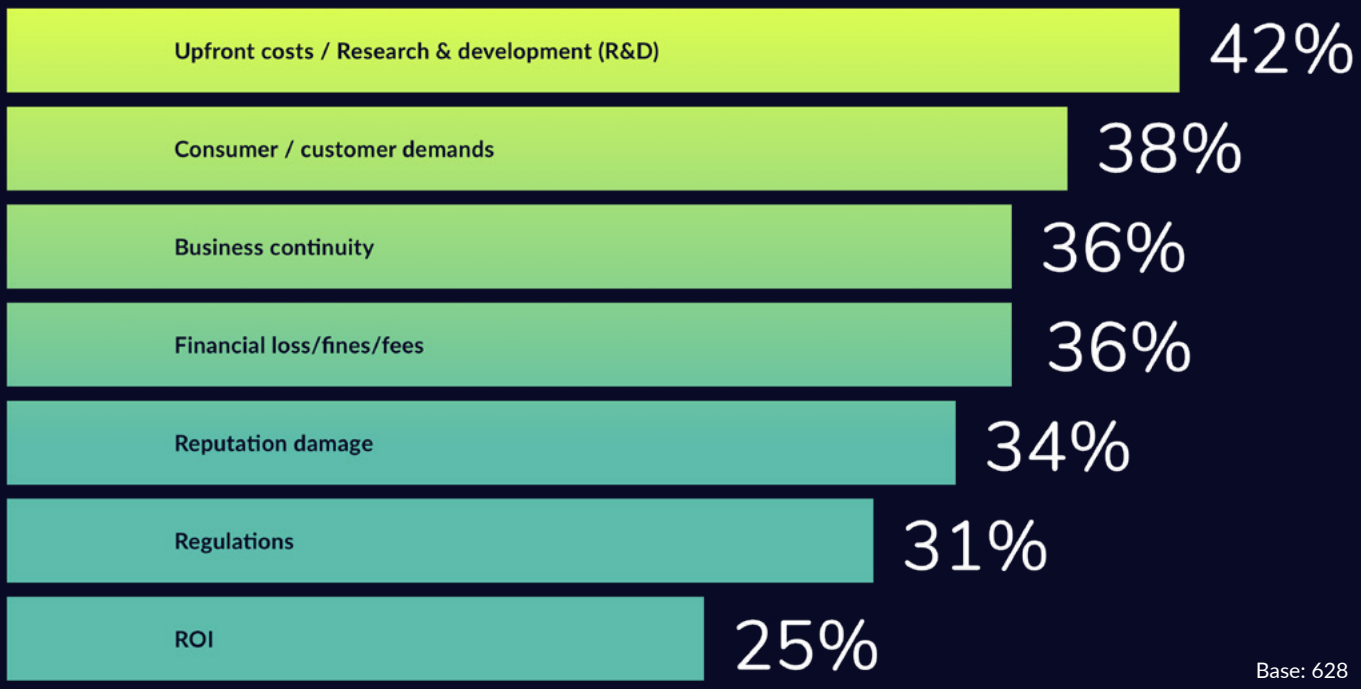
half of responses consider the additional cost of security to be a top barrier to improving it

42% Base: 628

2 in 5 believe upfront costs and R&D to be a top issue

This offers a key insight into what is driving manufacturers: the cost per unit remains pivotal to their success

What are the most pressing issues when you think about security?



Base: 628

Similarly, of the survey respondents who felt that their organization was unprepared to invest continuously in security:

- **40% cited "unstable market/economic conditions" as the key contributing factor**
- **54% cited "uncertain on ROI" and "lack of buy-in"**

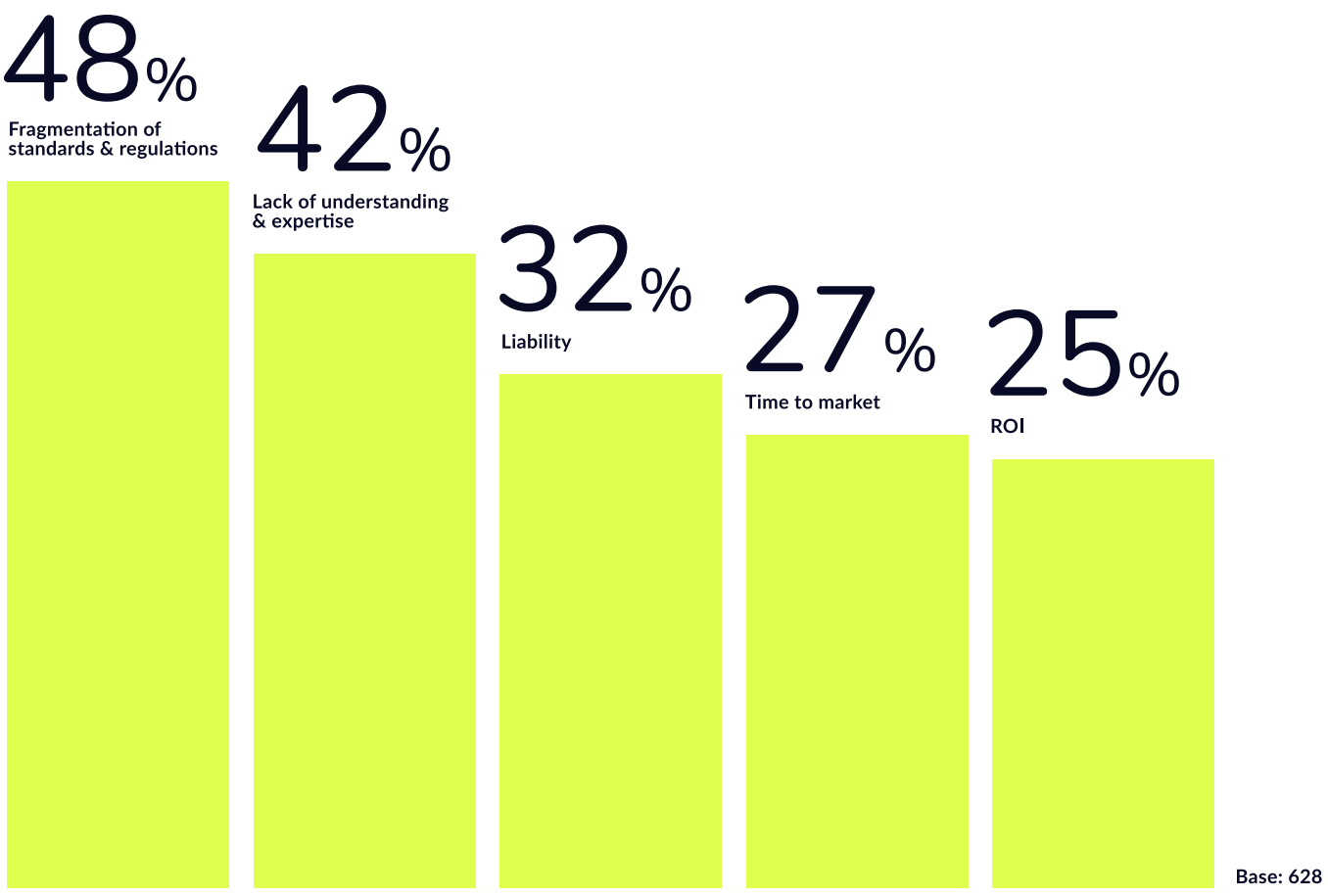
Respondents from Taiwan – a key part of the global supply chain commanding some **4.2% of the total IoT market share** – offer an interesting proof point, showing the highest proportion of respondents not prioritizing security requirements (7%). Again, the reason cited was mostly on the grounds of cost, showing again that traditional OEM thinking around making every penny count tends to devalue security as a whole.

The good news is that four in five respondents overall do feel at least 'quite prepared' to spend continuously on security for tools and resources, however, this continuous spend is often supplementary to a lack of up-front security planning (such as threat modeling which we'll cover later).

The other main barrier highlighted by our results is the fragmentation of standards, seen as a top challenge by 48% of respondents, while 42% cite a lack of understanding or expertise within their business.

> "Security is a cost. However, it's also an opportunity for a competitive advantage. Security is less costly when you build it in at the beginning, instead of trying to bolt it on later."
>
> **Fabio Vignoli, Head of Product Security at Signify**

What do you consider to be the biggest challenges with regards to IoT security?



Almost half consider the fragmentation of standards and regulations as a top challenge for IoT security (48%)

As the threat of insecurity grows and more hacks take place, it's only natural that governments and industry bodies are creating lots of different guidelines offering a variety of definitions for what 'best practice security' really means. It's not a surprise that this growth in solutions and approaches are creating the fragmentation cited in our results. Furthermore, 3 in 4 tech decision makers think governments should play a part in a guideline-development process for IoT security, demonstrating that government involvement is welcomed to help drive consistency across guidelines, reducing fragmentation.

For manufactures in the field, it takes a lot of time to evaluate the different solutions and approaches to security, which can slow down both product development and market adoption. To bridge this gap, common languages and a unified approach across standards will become even more critical.

What Does the Current Regulation Landscape Look Like?

In response to the IoT cybersecurity threat, governments and regulatory bodies around the world are taking action and introducing a number of regulations, guidelines, and laws, such as **ETSI EN 303 645** and **NIST 8259A**.

However, these local guidelines and regulations typically mandate a baseline of critical IoT security and varied wording and requirements bring new challenges. In a global economy, companies are forced to navigate regional differences in regulations and create global solutions with local conformance.

The good news is that the regulatory baselines are in fact well defined and aren't drastically different beneath the semantics. They share common goals: the adoption of good security practices, trust, and to assure consumers their devices are built upon security foundations.

Threat Modeling Adoption

47%

of respondents are carrying out threat analysis for every new product they are creating and in smaller companies this percentage drops to 33%

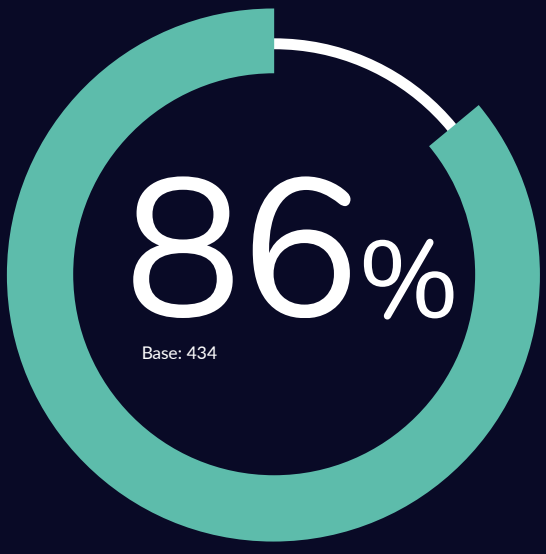
Despite the mainstream hacks and statistics mentioned earlier, an alarming fact is that in our survey, only 47% – under half – said that they carry out a threat model in the design of every new product. Being a critical component of security design, this number isn't high enough and perhaps represents why hacks and vulnerabilities are so common. This is another area in which the company size has an effect on things, again showing a need to democratize security to enable best practice security analysis and implementation:

In smaller companies (1-49 employees) the percentage drops to

33% Base: 434

In larger companies (5000-9999 employees) the percentage rises to

67% Base: 434



Although the notion of threat modeling sounds simple, it's actually a complex process that takes security expertise to carry out. We now know that threat modeling has historically been skipped during the production process for many connected devices. Seeing examples and receiving training in this area are likely to be key enablers for manufacturers to enable IoT security to scale.

The good news, however, is that the majority of respondents (86%) say it's likely they will relook at threat analysis on products that have already been released. To us, this perhaps suggests that – on realizing that their security practices aren't currently up to scratch having answered the first question - respondents then decided that they would reevaluate protocols on their existing products as a result. Or it might show us that, as IoT devices become mainstream enough to warrant more attempted attacks, early decisions are only now being reevaluated.

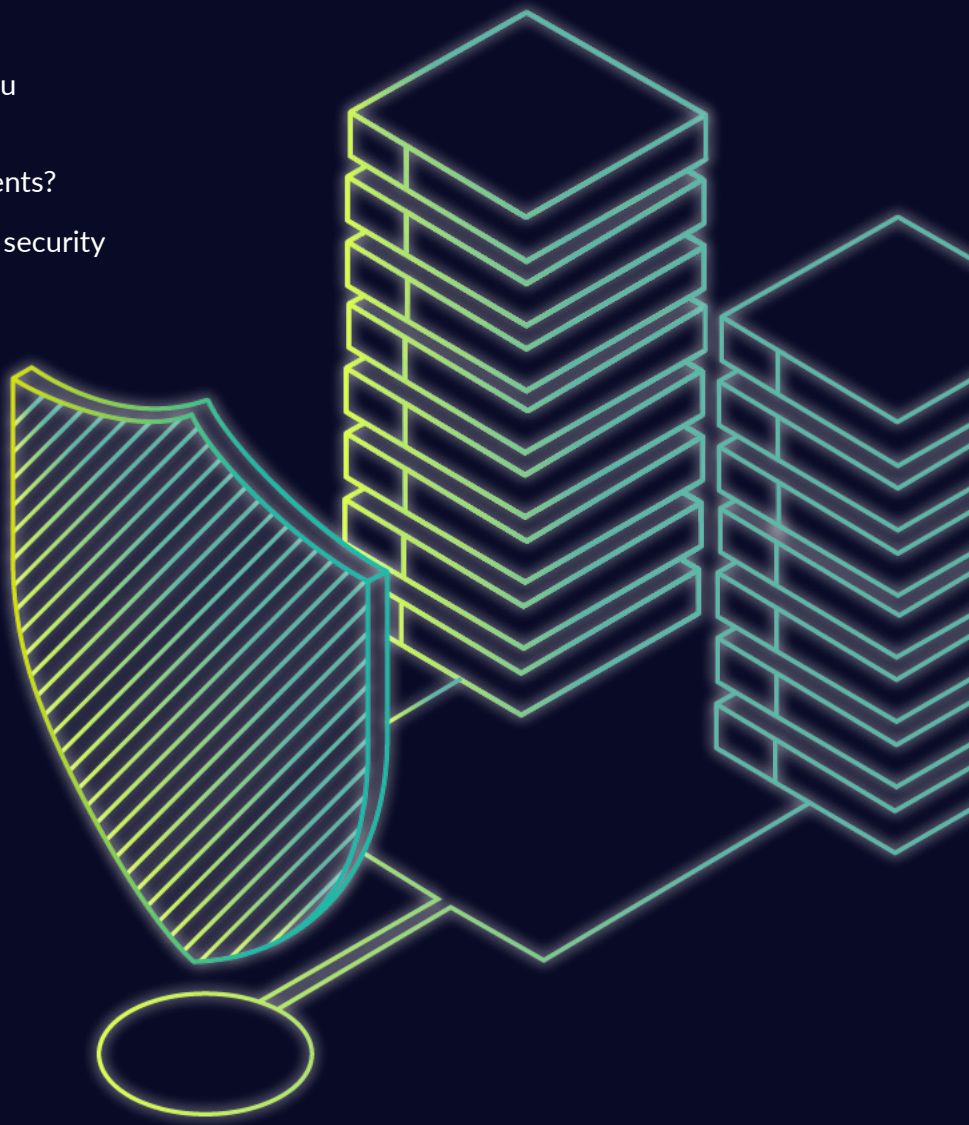
What is Threat Modeling and Why is it Important for IoT?

If you don't know what you're protecting against, how do you know how much security you need? To design-in security, developers and manufacturers should start by analyzing the way the device will be used in its intended application, and documenting the ways each device could be attacked. This is a process known as Threat Modeling.

The resulting Threat Model will highlight critical issues you need to address and challenge you to consider important questions, such as:

- What are your most valuable assets?
- What are the potential threats to your device?
- What type of attack do you need to protect against?
- How severe are the threats?
- What counter-measures could you implement?
- What are your security requirements?
- How does your device meet your security requirements?

This process will help you decide how robust your security needs to be and what, exactly, you need to do to protect your IoT product. It will help you determine the right level of security for your device, meaning you will not be over-spending or exposing your device, your organization or your customers to unnecessary risk.



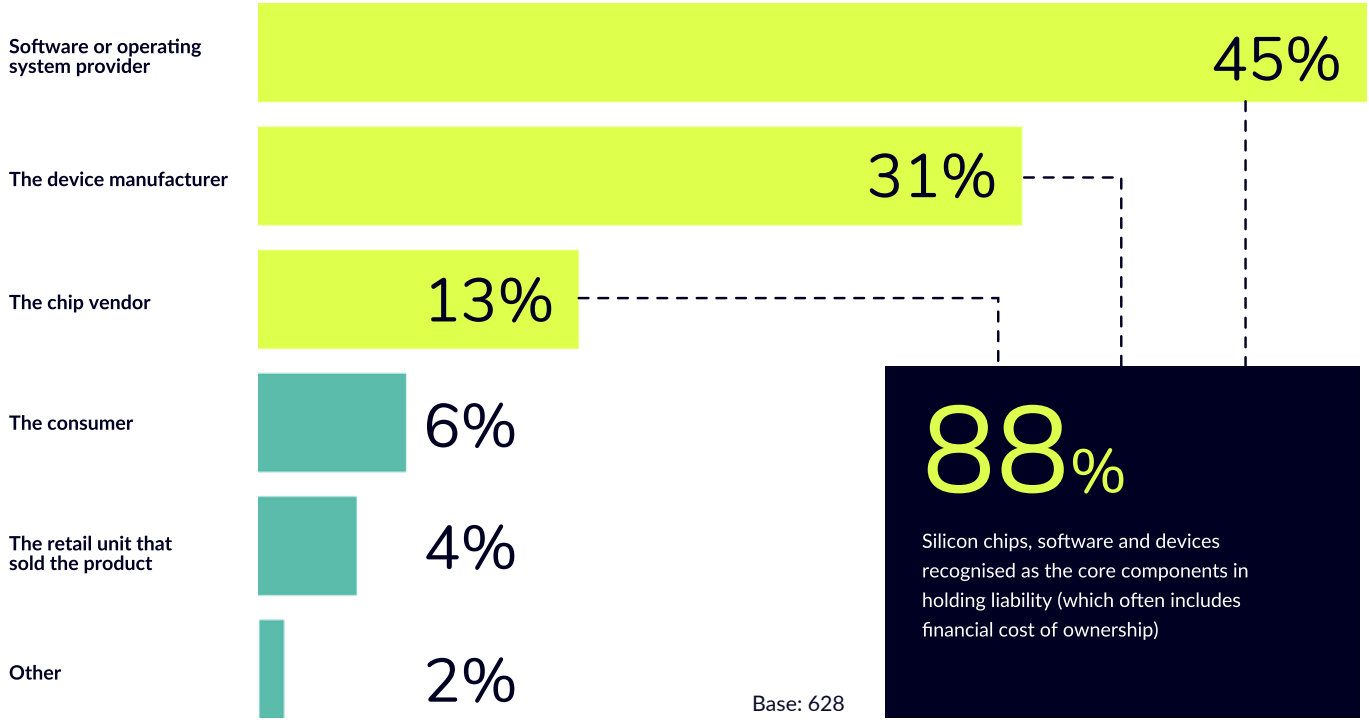
Where Does Security Responsibility and Liability Lie?

When we talk about the risks associated with IoT, an interesting talking point to cover is liability. Ultimately, where there are hacks and vulnerabilities, there is liability – someone is responsible for the "cost of failure" and carries the financial burden.

When we look at historical hacks, it's very common that the hack originates from software vulnerabilities. However, as we move towards digital transformation, it's clear that the relationship between hardware and software is critical and all areas of the value chain need to play their part in securing IoT. As we move to a hardware-based RoT in devices, the issue shifts to ensuring that the software is correctly utilizing RoT secure services. Building a strong hardware security foundation (on which the software and device applications can leverage security functions) creates layered, ultimately more robust security. The role of the whole technology industry is reflected by our study that found 89% of respondents place liability on the silicon, software and device manufacturers rather than consumers and retailers. Ultimately, the ecosystem must work together to provide layered security: reducing hacks and allowing us all to innovate.

The good news is that the importance of secure hardware is being recognized. Of those surveyed, 9 in 10 tech decision makers believe secure hardware components are important for realizing digital transformation, which is a positive trend towards understanding the importance of – and route to – more secure devices.

In your view in the case of a security failure, where does the liability lie?



Bridging the Gap

Summary

As we look at how we bridge the gap two things were highly ranked across our respondents: the role of certification and the importance of collaboration. Certification offers the industry a way to benchmark their security implementations, gaining assurance that they are doing the right things – yet a high percentage of our respondents are skipping using external labs. The second element is collaboration, which is overwhelmingly sought by those in the industry, showing a strong desire for OEMs and software vendors to navigate the issues of cost and fragmentation together.

Building on a common foundation of security and collaborating on the implementation of security measures that save both up-front and longer-term costs. These along with alignment of legislation and standards will democratize the security landscape making best practice security a standard and enabling the industry to scale.

The Role of Certification

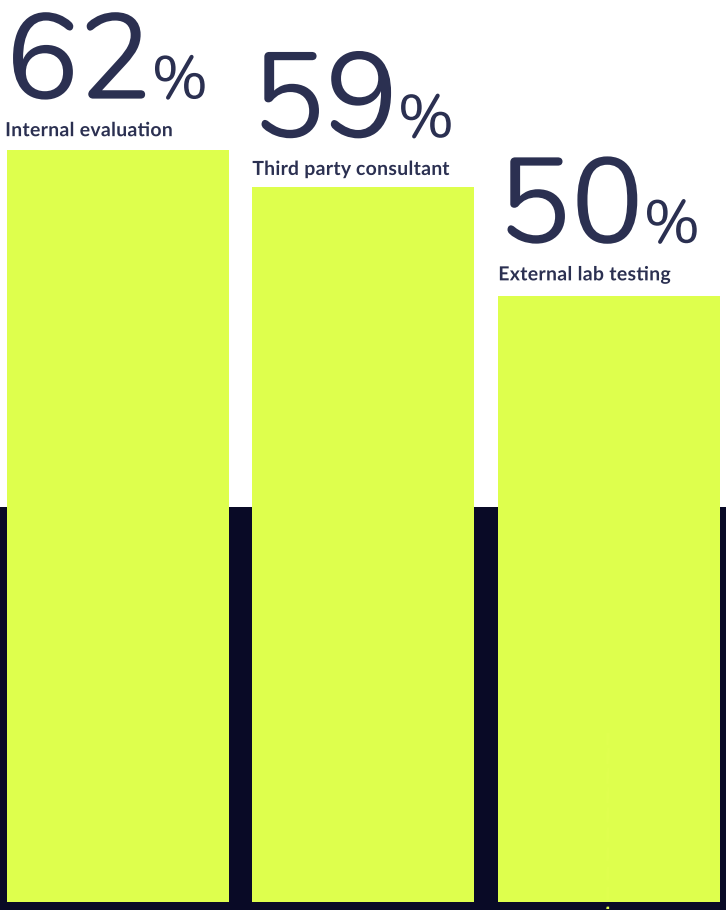
When we look at testing security implementations and their robustness, different companies have different strategies that sit in three categories: internal evaluation, security consultants, or evaluation with external labs. In reality, third-party evaluation should be the preferred approach as it offers additional objective measurement of a product's integrity and assurance that the product conforms to the security standard or specification it is measured against.

However, when we review the data in our report, 3 in 5 respondents (62%) say their security team certifies their security implementation internally, which points to a market of isolated developments and disparate, proprietary solutions.

Company size plays a factor here too, the percentage that makes use of external lab testing drops to 44% in companies sized 50-249, compared to 73% for larger companies of 5000-9999 employees. This highlights again the disparity in security resources facing smaller companies.

This is worrying: we need to ensure that we are measuring how robust our security implementations are, otherwise, you can never truly know if you're doing the right things. It comes back to our initial findings at the top of this report, 61% believe we're "on track" with security – but without third party evaluation, you can never know for sure.

How do your engineering teams certify their security implementation?



Base: 434

External lab testing

44% Base: 434

make use of external lab testing in companies with 50-249 employees

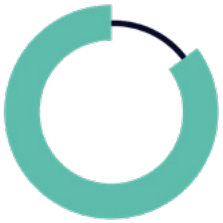
73% Base: 434

make use of external lab testing in companies with 5000-9999 employees

A Collaborative Future

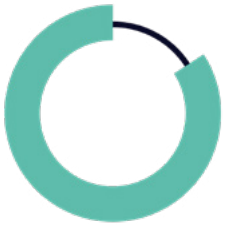
A combined 93% of our survey respondents reacted positively to the suggestion that collaborative, common certification can be a differentiator in the market, while 85% of survey respondents stated an interest in industry collaboration and cross-market knowledge sharing around IoT security. On top of this, 84% of tech decision makers show interest in the development of an industry-led set of guidelines and processes to help build IoT security. In other words? There is an appetite for a standardized approach to bridge the gap between security challenges and expectations.

Collaboration is Needed & Welcomed



85% Base: 628

would be interested in industry collaboration and cross market knowledge sharing regarding IoT security



84% Base: 628

of tech decision makers would be interested in an industry-led set of guidelines and processes to help build IoT securityoyees

At PSA Certified, we believe this kind of collaboration is the primary way forward for security implementation across the value chain, but this is not just opinion; it's a need we see crystallizing among a raft of seemingly disparate industry influencers and industry verticals. There are many ways to collaborate including:

- Identifying industry bodies who are collaborating and sharing best practice that you can follow.
- Identifying standards or guidelines built by experts that reduce your investment needed in security.
- Playing your part and support the ecosystem in adopting a common standard and language for security.

One of our biggest insights into this need for cross-industry collaboration is evidence of siloed security development. Collaboration on a common Root of Trust and measurement of security through certification is key to minimizing the core security challenges facing OEMs: cost, fragmentation, and bridging the gap between security perceptions and reality.

> "Regulations are ramping up more and more, so you really don't want to go it alone! When things go wrong with security (and they always will go wrong) you don't want to be on your own. Be part of the herd and don't be left behind."

Brad Ree, CTO IoXT Alliance put it in an episode of our #beyondthenow podcast

Redefining IoT Security to Bridge the Gap

With all of this in mind, how do we bridge the gap to find solutions to the key challenges? The **PSA Certified founders** are passionate about the two key areas we've been discussing: democratizing security and reducing fragmentation. The key is finding a unified approach to security, which helps companies of all sizes to implement a security baseline and we've been collaborating as the PSA Certified founders and the wider ecosystem to make that happen.

The **PSA Certified security framework** is developed by industry experts in the security field and offers a path to certification aligned to major IoT security standards, regulations and guidelines. This enables silicon providers, software providers and OEMs to demonstrate and showcase their security credentials. 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 OEMs, purchasers and consumers by solving issues around fragmentation through collaboration. Plus, 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

Our partners are both validating and helping shape that vision. We're delighted that we've been seeing significant momentum on a unified PSA-RoT implementation with silicon vendors, plus software and manufacturers joining the mission. If you want to learn more about the PSA Certified program and find ways to collaborate, **contact us**.

Conclusion

As the world embraces digital transformation, more and more connected devices come online each day. The increased appetite for hacking devices has made security an essential part of a product's development, rather than the afterthought it's sometimes been seen as in the past.

In this report we've uncovered some grounds for optimism: OEMs are now, increasingly, aware of the importance of a Root of Trust, and the how security implementation can improve their products and services. We also see hugely positive trends in collaboration where not only is collaboration demonstrably sought by decision-makers in the industry, but it's also recognized as a key way in which security fragmentation can be mitigated.

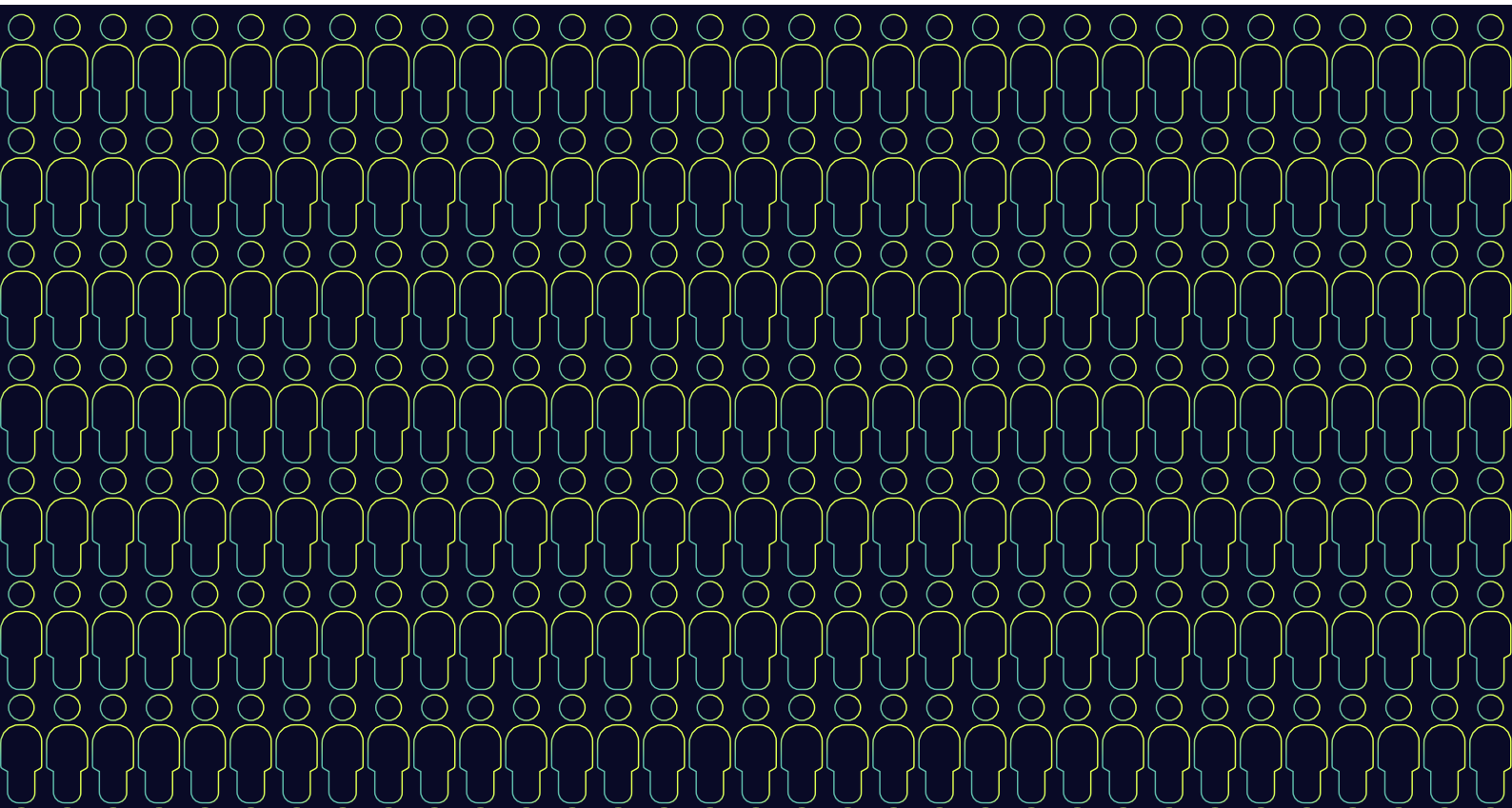
In other words: fostering a connected-devices industry that embraces collaboration in the security space – of the kind made possible by PSA Certified – will reduce costs, reduce doubling-up on work, and ultimately free up historically misspent resource for other, exciting areas of companies' digital transformation.

However, despite trends in a positive direction, this report highlights a gap between perceptions and reality in IoT security best practices – one where the ecosystem thinks we're ahead of the challenge, when in fact the number of hacked devices is only increasing. We also highlighted some key gaps and patterns that affect most businesses, regardless of industry: technological fragmentation, and the difficulty in mapping cost against a perceived result – especially in smaller companies. Confounding this is the misperception that the associated costs will outweigh any possible security gains and the fact that a surplus of differing approaches has added bloat to the security implementation process.

If we're truly going to realize the true potential of digital transformation, it's clear that we need to overcome the risk of fragmentation, align to regulation and reduce some of the cost burdens that comes hand-in-hand with security. There is no denying that these are big challenges to bridge – but now the challenges are known, it gives us a path in the right direction.

Collectively we can work together to reach the potential of digital transformation - and now is the time to take action.

Overcome the barriers to IoT security with PSA Certified



Methodology

The core of this report's findings originate from a November 2020 survey conducted among 628 Technology Decision Makers in the UK, US, Germany, France, China, Taiwan and Korea by Sapio Research.

The majority of interviews (570) were conducted through an online panel by Sapio Research in November 2020 using an email invitation and survey link. The remaining interviews were reached out to by Arm over email and social media (58).

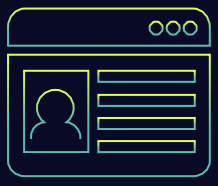
Three types of responders were selected:

- Design and manufacturers of products and components of IoT products & services
- Retail and distribution of IoT products or services
- Analysts and consulting companies, of any size

Total respondents: 628

Country of residence:

Great Britain: 100
America: 130
Germany: 96
France: 98
China: 93
Taiwan: 38
South Korea: 73



Audience

39% from Design & manufacture of products and components of IoT product & services

31% from Retail & distribution of IoT products or services

31% from Analysts & Consulting companies, of any size

Role type

25% of respondents held C-suite/Executive level positions

36% of respondents held Director level positions

40% of respondents held Manager level positions

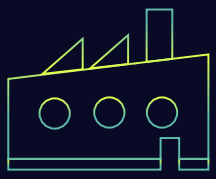
Size of company

1 to 249 of employees : 27% of respondents

250 to 999 of employees : 33% of respondents

1000 to 9999 of employees : 31% of respondents

10,000+ of employees : 10% of respondents



Business sector

27% of respondents from Tech sector

27% of respondents from Retail & Distribution sector

24% of respondents from Professional services sector

At an overall level results are accurate to ± 3.9% at 95% confidence limits assuming a result of 50%. When looking at only panel responses, results are accurate to ± 4.1%. Client only responses - where herein incorporated - are accurate to ± 12.9%, given the significantly lower base number.

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

psacertified™