THE IOT TRUST DEFICIT

A Data Report on Consumer Confidence in the European Market

Survey Results & Analysis for
IoT Product Leaders, Innovators,
and Policymakers

September 2025

TABLE OF CONTENTS

salt& pepper

IoT in Europe is At a Crossroads

The European IoT market is expanding fast, but innovation doesn't automatically translate into adoption. Founders and product teams face recurring obstacles: consumers hesitate to trust, regulations keep shifting, and technical complexity slows down launches.

At Salt & Pepper, we've learned that building connected products isn't just a technical challenge—it's a business model challenge. Hardware, software, compliance, distribution, device partners: every layer comes with interdependencies. Juggling them right is critical for survival and growth. A great device without interoperability fails. A brilliant app without reliable hardware partners stalls. A compliant product without the right go-to-market never scales.

It's clear: successful IoT companies don't just build products. They **orchestrate ecosystems that work as business models.**

This is where our passion lives when we step in as a product partner. Over the past decade, we've worked alongside startups and scale-ups to design, build, and launch IoT solutions that earned user trust, passed regulatory tests, and, most importantly, reached viable, scalable business models.

What we've seen is consistent. Trust drives growth, and visible privacy and security are essential. Early regulatory compliance builds credibility with users and investors. Seamless cross-ecosystem functionality is rewarded, while AI can enhance safety and personalization if kept transparent and user-controlled. Ultimately, adoption depends not just on the device itself but on the surrounding business models, partnerships, and services.

We started this research initiative with a pressing question: what happens (for consumers and for businesses) when two strong forces reshape the IoT space at once: AI and cybersecurity? To answer it, we combined the voices of 1,200 European consumers with those of ecosystem players across industries.

The result is a first-hand, data-driven look at what drives adoption, what blocks it, and where trust, AI, and cybersecurity will reshape the IoT market in Europe.

Based on these insights, Salt & Pepper is more committed than ever to being a product companion for IoT innovators in Europe, helping them solve technical complexity, navigate dependencies, and design sustainable business models. Our mission is simple: to help ambitious IoT teams build connected products that survive, scale, and make everyday life safer and better for their users.

What's more, we believe the opportunity is uniquely European. Europe can become the strongest player in the global IoT market, with a distinctive combination of safety, usefulness, and sustainability. If we put trust and seamlessness at the centre, European IoT products can set the global standard: secure by design, built for real human needs, and aligned with long-term responsibility.

That's the future we want to help build.

Cristin Iosif
CEO Salt & Pepper

From 'Smart' to 'Seamless:' What Do European Consumers Really Want?

The European Smart Home market is no longer an emerging niche; it is a mainstream powerhouse. In 2025 alone, the market is projected to generate $44.8 billion in revenue, placing Europe at the forefront of the global smart home revolution. This is just the beginning. With a forecast annual growth rate of 9.03%, the market is expected to surge to a projected volume of $63.3 billion by 2029. This financial growth is mirrored in our daily lives. An estimated 77.9% of European households will utilize smart home technology this year, a figure on track to reach near-universal adoption at 96.8% by 2029.

But behind the market growth statistics lies a more complex human story. Adoption is not guaranteed. For every enthusiastic early adopter, there is a skeptical consumer holding back. Why?

To tackle this conundrum, Salt & Pepper surveyed 1,200 consumers across four key European markets—the United Kingdom, Germany, the Netherlands, and Denmark. Our goal was to move beyond technical specs and understand the real-world drivers, frustrations, and fears shaping the future of connected living.

This report is a transparent, comprehensive look at our full survey results. It is a strategic guide for those building the future, designed to give product teams, founders, and policymakers a direct view into the mind of the European consumer. Inside, you'll find the data, the analysis, and the insights needed to build the next generation of IoT products that consumers will not only use, but trust.

The Key Insights:
A Market at a Crossroads

The Entertainment Gateway:

Smart TVs and sound systems are the primary entry point into the smart home for a commanding 70.3% of consumers, making it the most mature and accepted category.

The Trust Wall:

For those who haven't adopted smart devices, it's not about price. Distrust in privacy and security is a primary barrier, cited more often than cost or a perceived lack of need.

The Certification Imperative:

An overwhelming 81.1% of consumers would be "definitely" or "maybe" more inclined to purchase a device with an official EU cybersecurity certification label. Regulation is not a burden; it's a consumer-demanded feature.

The Usability Gap:

For current owners, the daily experience is fraught with friction. Top frustrations include unreliable connectivity, software glitches, and a lack of interoperability between different brands.

The AI Dilemma:

Consumers see the future potential of AI, with their biggest hope being enhanced security (30.5%). However, this is tempered by their biggest fear: that AI will introduce new security risks (27.3%).

salt & pepper

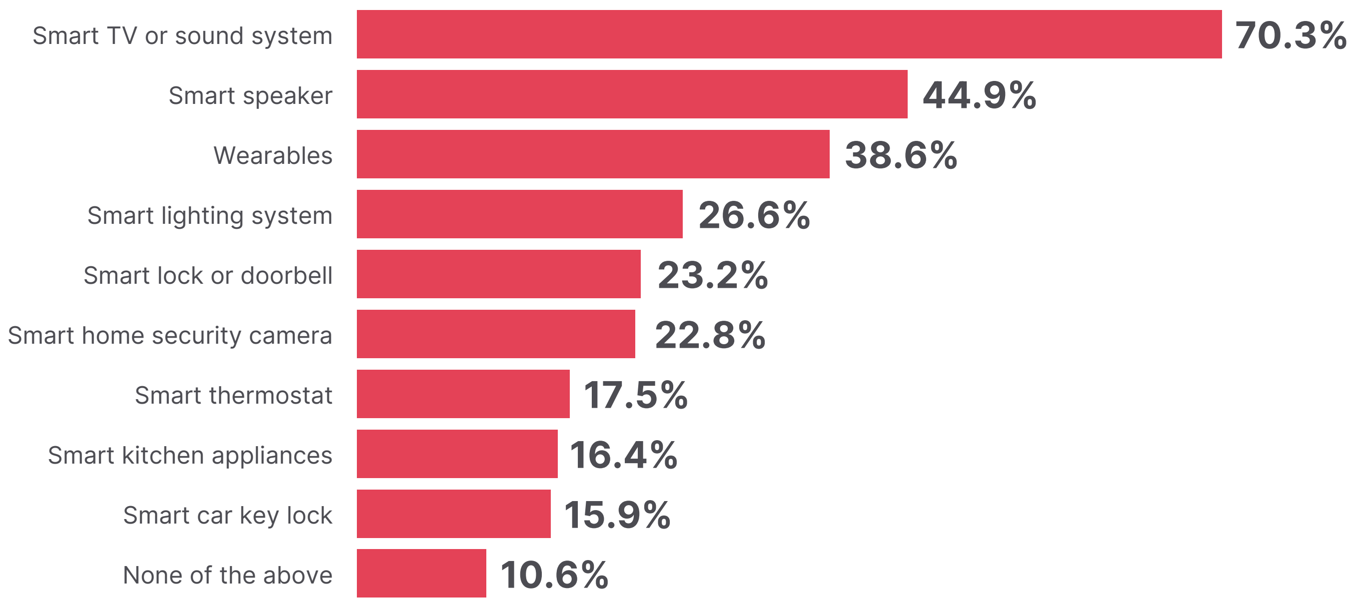
CHAPTER 1

The European Smart Home Landscape

Who Owns What, and How Do They Use It?

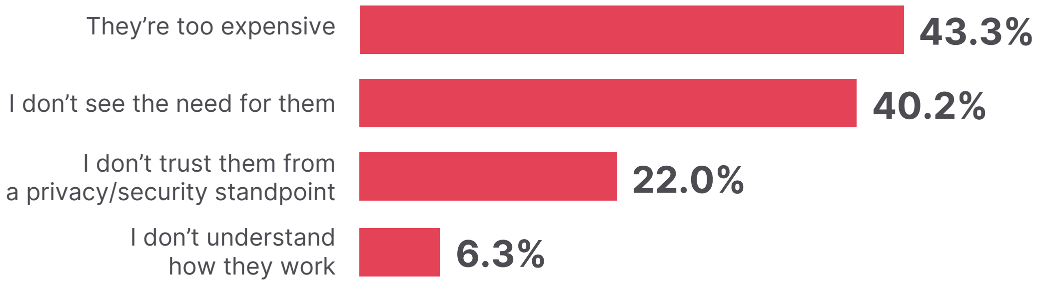
To understand the market, we first need a clear picture of current adoption and usage patterns. Our data reveals a landscape dominated by entertainment devices, with high user engagement but clear motivations centered on convenience and security.

Q1: Excluding smartphones, which of the following smart devices do you currently use?



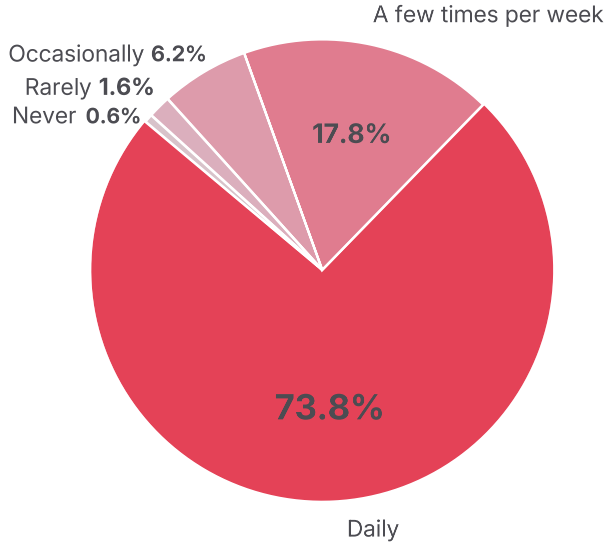
Insight: The dominance of Smart TVs highlights that the initial entry into IoT is often passive, driven by a core entertainment need rather than a desire for a fully integrated smart home. The 10.6% who own nothing represent the key target for market growth.

Q2: What are the reasons you don't currently use any smart devices?



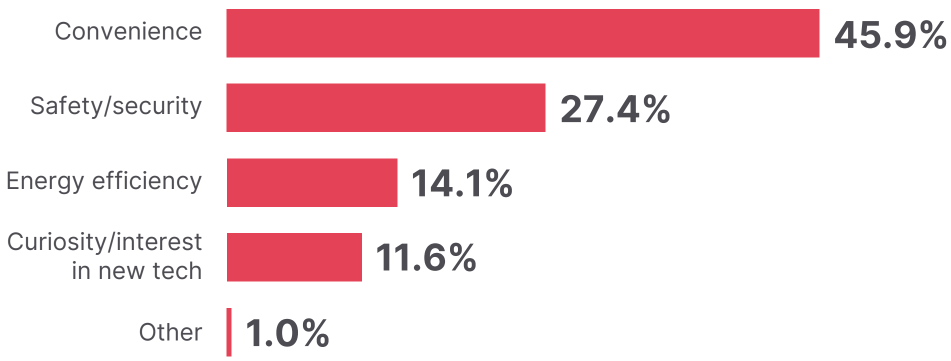
Insight: While cost and perceived utility are significant barriers for non-users, a fundamental lack of trust remains a critical factor preventing a substantial portion of this group from entering the market.

Q3: How often do you actively use any of your smart devices (excluding your smartphone/tablet)?



Insight: Once adopted, smart devices become deeply integrated into users' lives. The high level of daily engagement indicates that these products are successfully delivering on their core promise and are not mere novelties.

Q4: What is your MAIN reason for using smart devices?

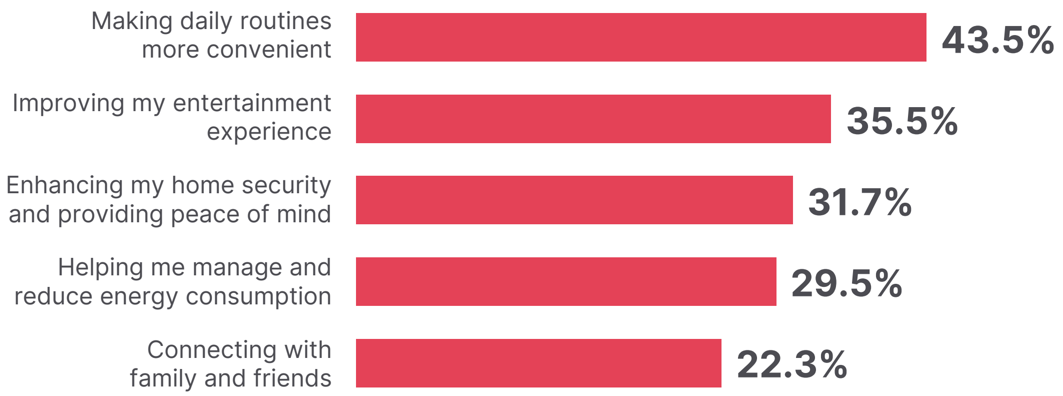


Insight: Convenience is the overwhelming driver for smart device usage. This suggests that the most successful products are those that seamlessly remove friction from daily routines. Security follows as a strong secondary motivator.

CHAPTER 2

The User Experience: Value vs. Frustration

Q5: In which of the following areas have your smart devices provided the most significant value or improvement?

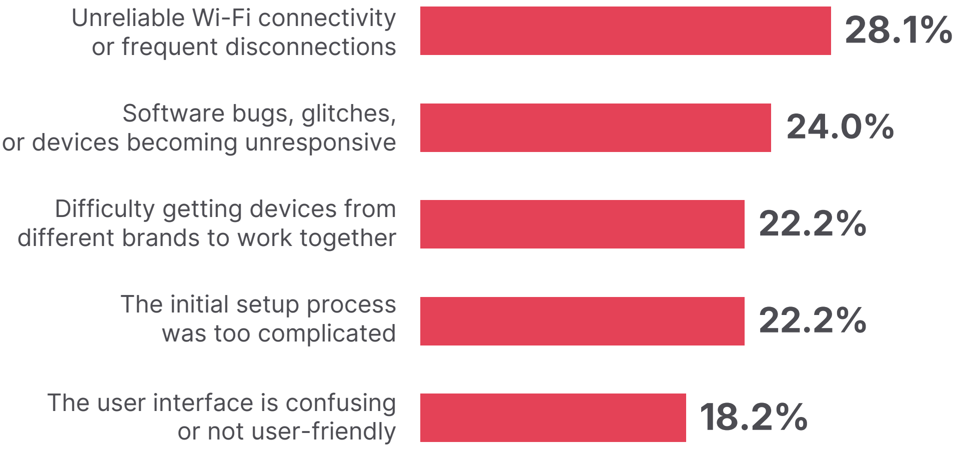


Insight: The perceived value aligns perfectly with the stated reasons for adoption: users feel their devices are delivering on the promise of convenience, followed by entertainment and security.

Smart homes shouldn't be about gimmicks or lock-in, they should be about giving people real control, privacy, and efficiency in their everyday lives. That's where we see the future of connected living in Europe.

– Stefan Witkamp, Founder & CEO Homey

Q6: What are the biggest challenges or frustrations you've experienced with your smart devices?

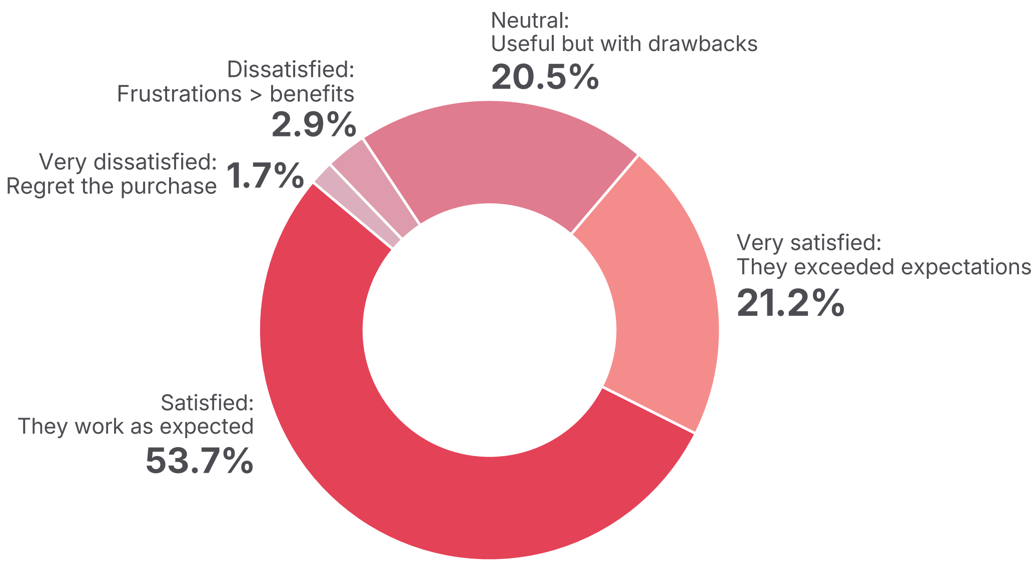


Insight: The top three frustrations are all technical and centered on reliability and interoperability. Consumers are tired of being their own IT support. The dream of a home that "just works" is being undermined by a fragmented and buggy reality.

The biggest barriers are trust and technical complexity — integrating multiple heating systems and meters requires patience, small pilots, and strong relationships with clients.

– Christopher von Gumppenberg, Co-founder & CEO, KUGU Home

Q7: Which statement best describes your overall feeling about your smart device(s) after owning them for at least 6 months?



Insight: Despite frustrations, the majority (74.9%) are satisfied. However, a significant one-fifth of users remain neutral, indicating that while the devices are functional, there is substantial room for improvement in the overall experience to turn them into enthusiastic advocates.

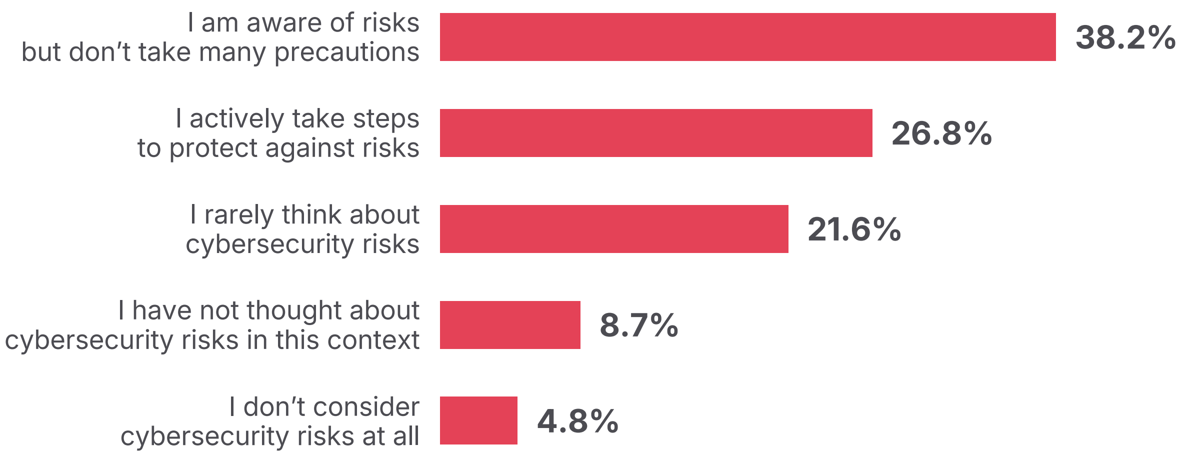
CHAPTER 3

The Trust Deficit

Deconstructing the Core Barrier to Market Growth

The greatest challenge for the IoT industry is not technology, it's trust. Our data reveals a deep-seated apprehension among European consumers regarding security and privacy, which actively suppresses market growth and user confidence.

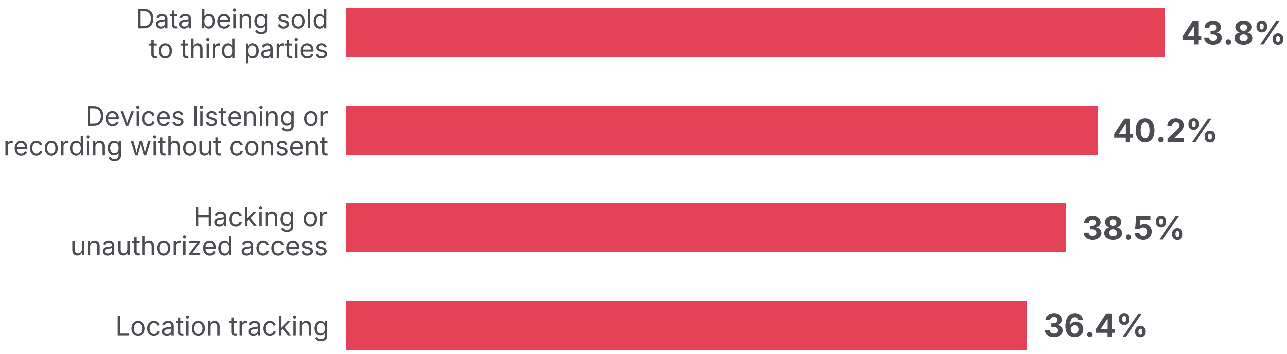
Q8: Which statement best describes your view on cybersecurity risks related to IoT devices?



Insight: While over a quarter of users are proactive about security, the largest group remains passively aware but inactive. This "Aware but Inactive" segment represents a major vulnerability and an opportunity for products that can offer automated or simplified security.

salt & pepper

Q9: Which potential risks, if any, do you consider when using smart devices?

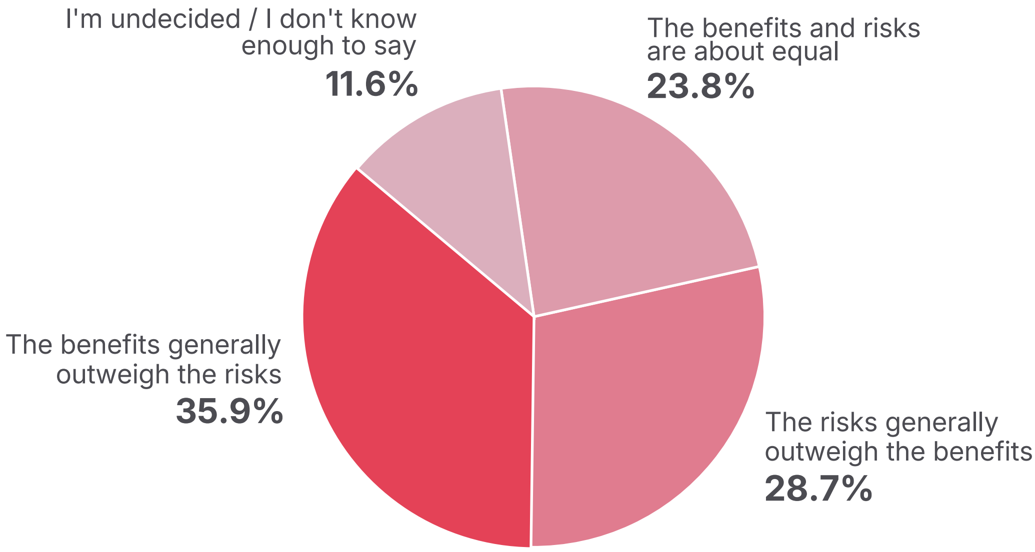


Insight: The biggest fears are not just about external threats like hackers, but about the actions of the companies themselves. The fear of personal data being monetized without consent is the top concern, highlighting a fundamental breach of trust between consumer and corporation.

The industry is still underinvesting in security because it's costly and continuous. Even with advanced protection, compromise is always possible, so detection and response are critical.

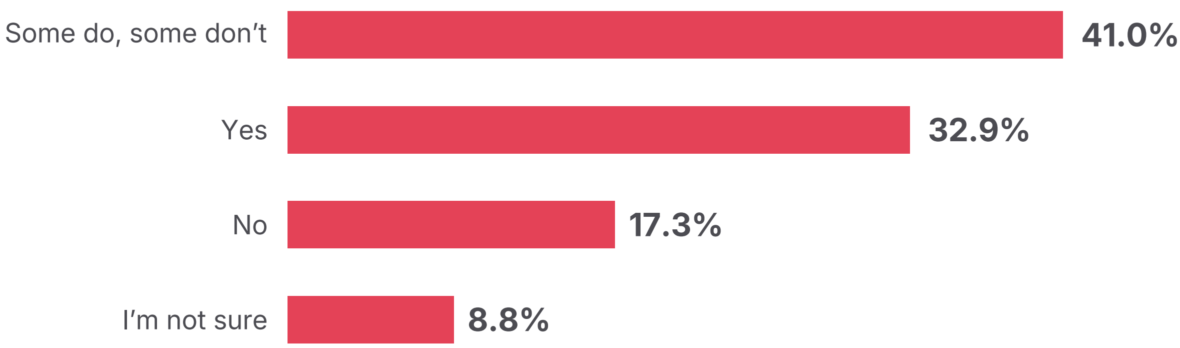
– Toby Wilmington, Co-founder & CEO, Periphery

Q10: When you weigh the benefits of smart devices against the potential privacy/security risks, which statement best describes your view?



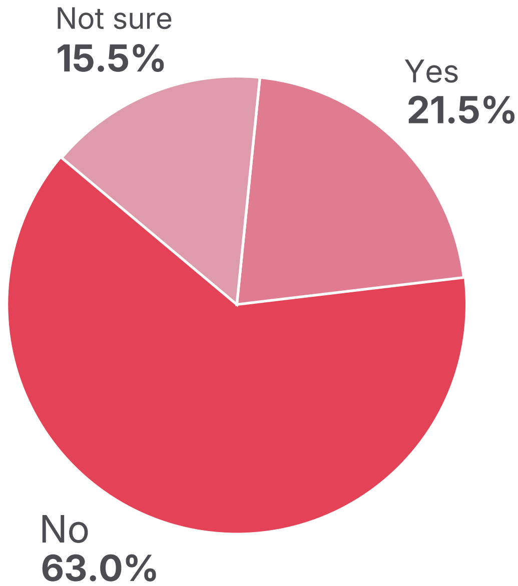
Insight: The market is almost evenly split. While a slight majority favors the benefits, over half of all users feel the risks are equal to or greater than the rewards. This precarious balance indicates that any significant security incident could easily tip the scales of public opinion.

Q11: Do you think smart device manufacturers do enough to protect consumer data and privacy?



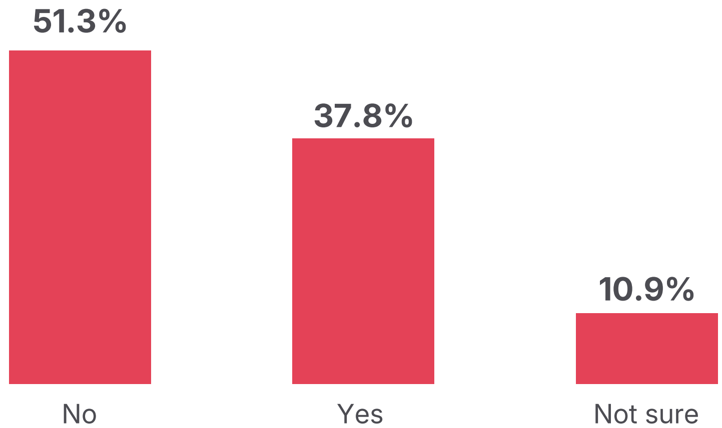
Insight: The industry has a trust problem. The dominant view that protection is inconsistent leaves consumers uncertain and skeptical. There is a clear opportunity for a brand to position itself as the undisputed leader in data protection.

Q12: Have you ever experienced or suspected a cybersecurity issue with a smart device?



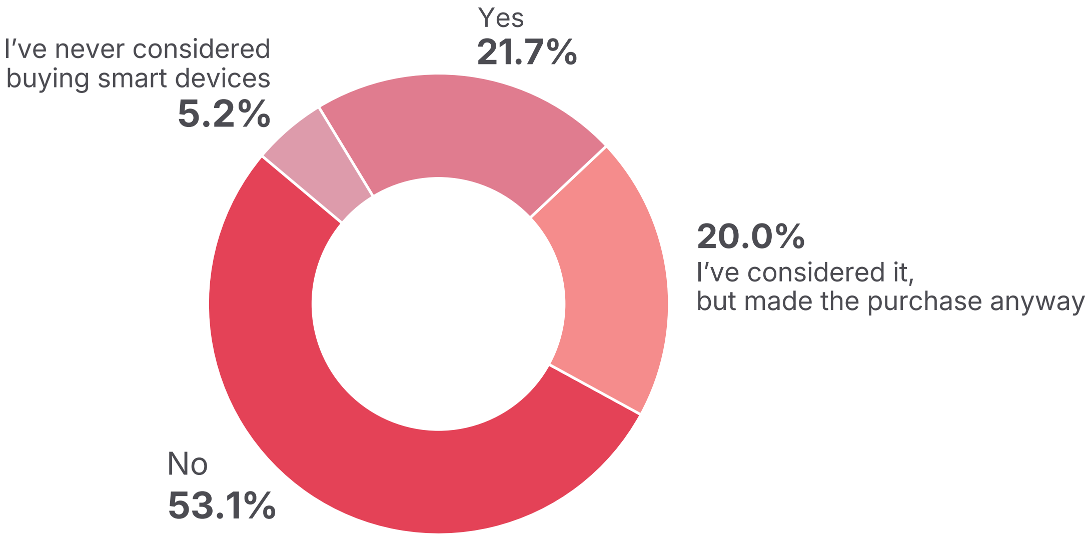
Insight: More than one in five users has personally experienced or suspected a security issue. This is not a theoretical problem; it's a tangible experience for a significant portion of the user base, which then fuels wider public skepticism.

Q13: Have you heard others (e.g., friends, family, media) talk about security or privacy concerns related to smart devices?



Insight: While direct experience is impactful, the narrative is also shaped by social circles and media. Over a third of consumers are hearing these concerns from others, amplifying the message of distrust far beyond those personally affected.

Q14: Have concerns about security or privacy ever stopped you from buying a smart device?



Insight: This question quantifies the financial impact of the trust deficit. For 21.7% of the market, fear has directly translated into a lost sale. Another 20% proceeded with a purchase despite their reservations, indicating a fragile and conditional trust.

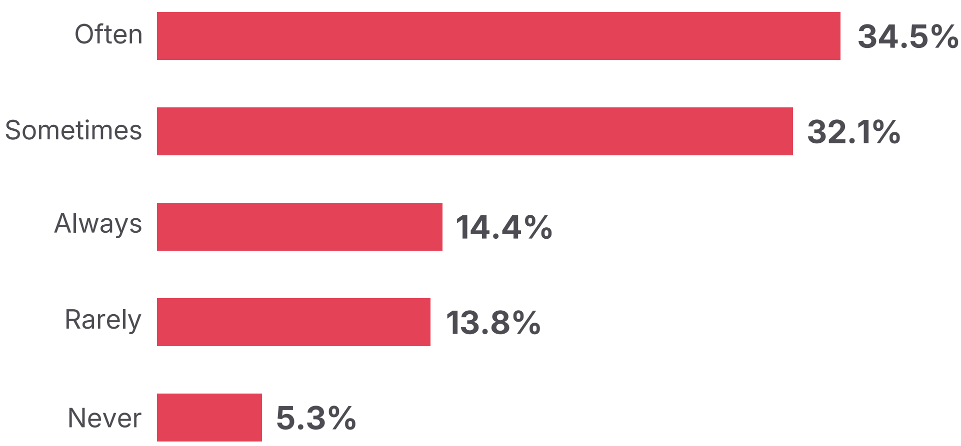
CHAPTER 4

The Path Forward: Building & Marketing Trust

A Consumer-Driven Roadmap for Growth

How can the industry bridge the trust deficit? Consumers have provided a clear set of instructions. They are actively looking for tangible signals of security, are willing to engage with privacy features, and place their trust in specific entities.

Q15: When purchasing a smart device, how often do you review its privacy or security features?



Insight: A combined 81% of users review privacy or security features at least sometimes before buying. This is not a niche activity. Privacy is a key part of the customer's purchasing journey and must be addressed with clear, accessible information at the point of sale.

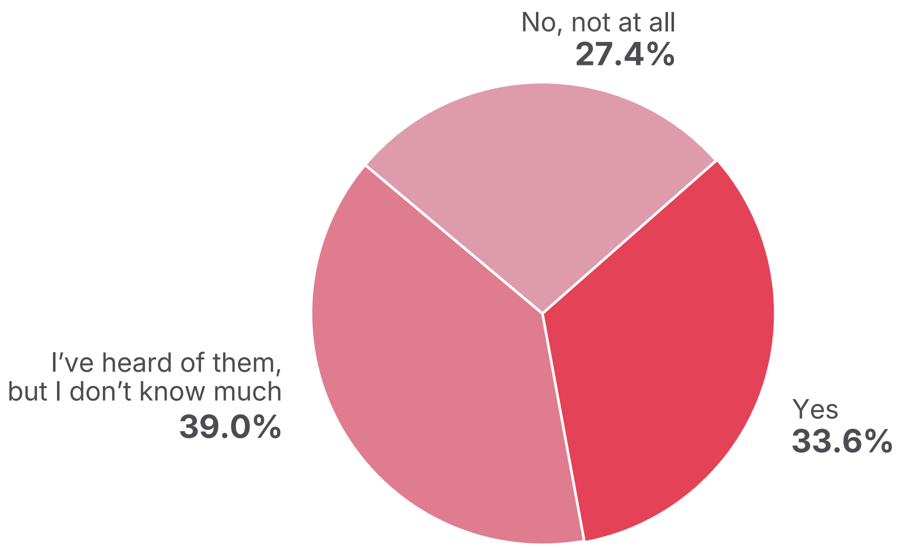
Q16: Rank the following groups based on how much you trust them to protect a user's privacy with regards to smart devices.

(1 = Most Trusted, 5 = Least Trusted)

Entity	Mean Trust Score
Device manufacturers	**2.82**
European regulators	**2.98**
Local tech companies	**2.99**
Big tech (Google, Apple, Amazon)	**3.28**
Internet providers	**2.94**

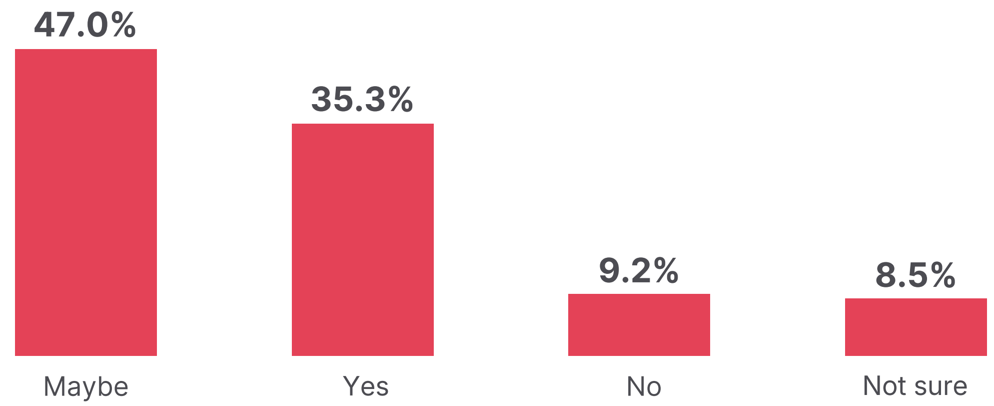
Insight: Consumers place the most trust (and responsibility) directly on the device manufacturers. They trust "Big Tech" the least. This puts the onus squarely on product companies to lead with trust, as consumers see them as the primary stewards of their data.

Q17: Are you familiar with any European regulations like the GDPR, AI Act, or Cyber Resilience Act?



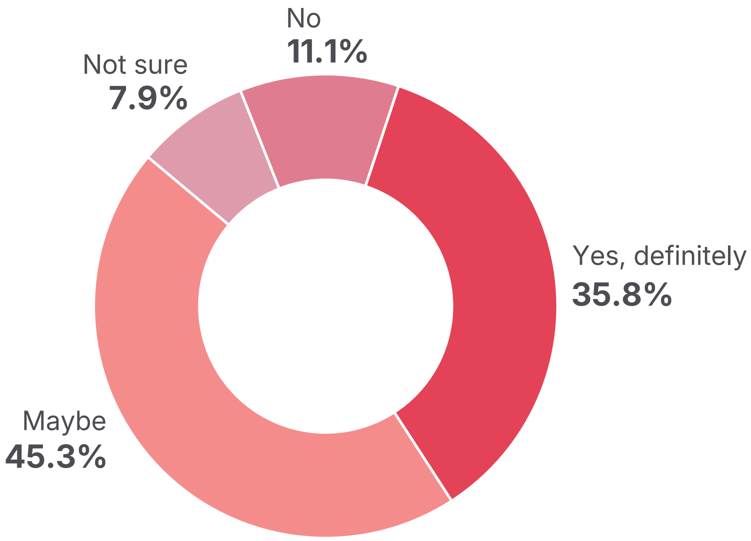
Insight: While a third are familiar, the majority of consumers are not experts on specific regulations. This means that simply being "compliant" is not enough; the benefits of that compliance must be translated into a simple, clear, and trustworthy signal for the average consumer.

Q18: Would you feel more comfortable using smart devices if they were developed under and fully compliant with strict EU cybersecurity regulations?



Insight: An overwhelming 82.3% of consumers see EU regulation as a positive factor for their comfort and safety. This confirms that a strong regulatory framework is a powerful tool for building consumer confidence.

Q19: Would you be more inclined to purchase a smart device if it had a certification or label showing it meets EU cybersecurity standards?

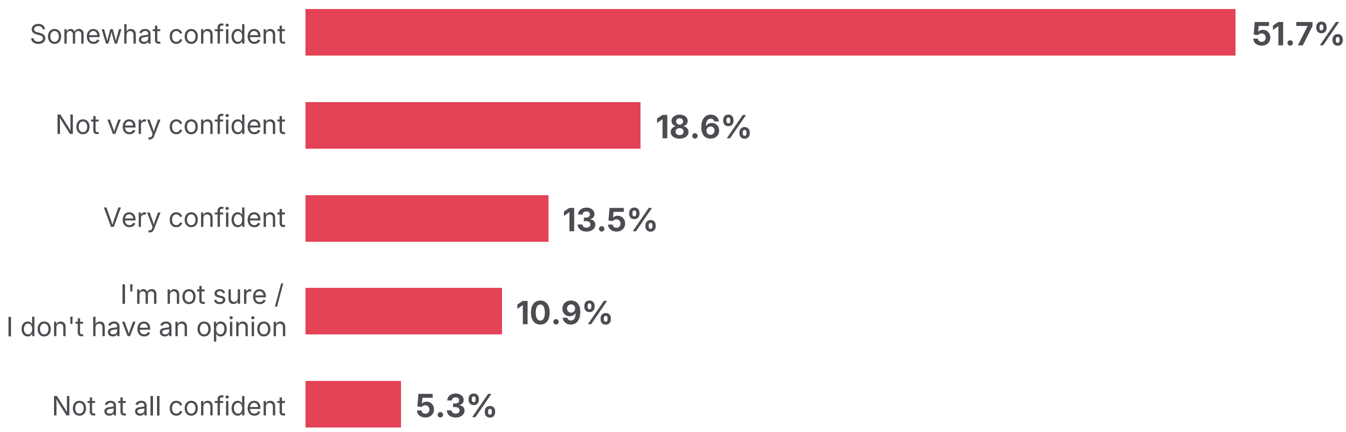


Insight: This is a crucial strategic finding. 81.1% of consumers are positively influenced by a trustmark. An "EU Certified" label is not a bureaucratic hurdle; it is one of the most powerful marketing and sales tools a company could ask for.

EU regulation sets a higher bar than the UK. For founders, the challenge isn't the standard itself, it's the clarity of the path to meet it.

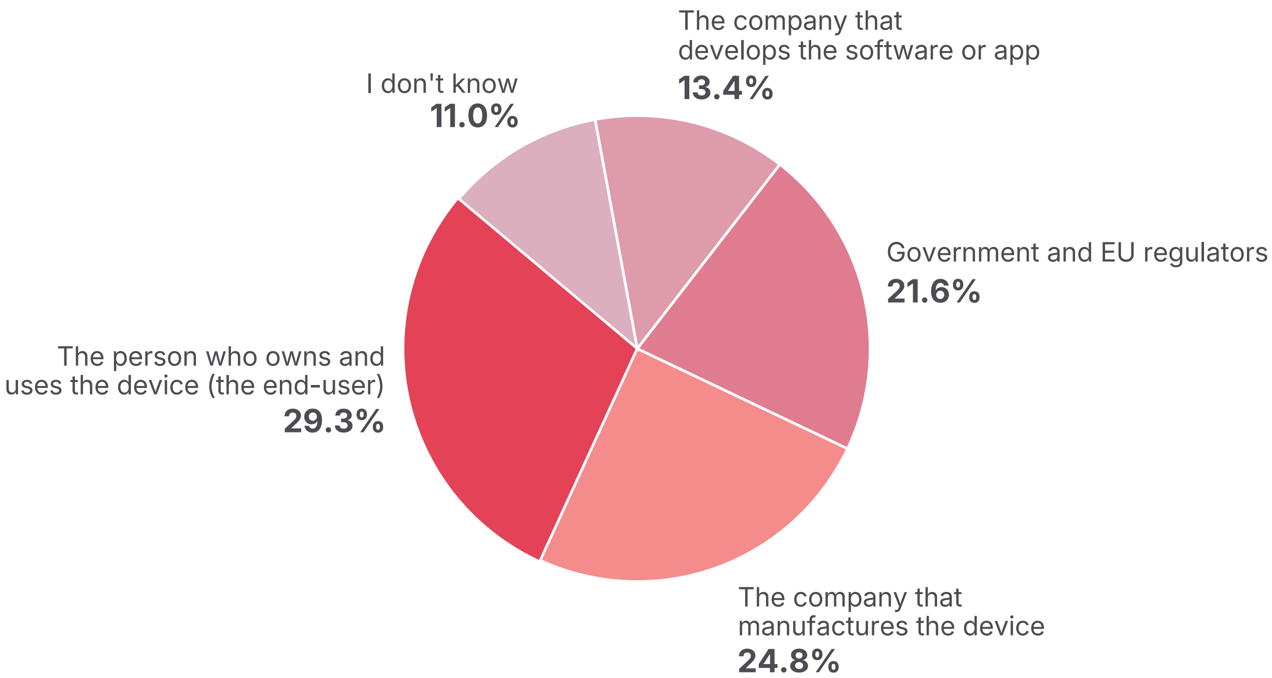
– Iyad Kayrala, Co-Founder & CEO of Vertassit

Q20: How confident are you that current EU regulations effectively protect a user's personal data when using smart devices?



Insight: Confidence in the current system is moderate at best. While consumers believe in the idea of regulation, they are not fully convinced of its current effectiveness. This creates an opportunity for certified devices to stand out as definitively secure.

Q21: Who do you believe should be primarily responsible for ensuring smart devices are secure?



Insight: Responsibility is seen as a shared ecosystem. While users accept a significant portion of the burden themselves (29.3%), they place nearly equal responsibility on manufacturers (24.8%) and regulators (21.6%). A successful security strategy must therefore empower users while demonstrating corporate and regulatory accountability.

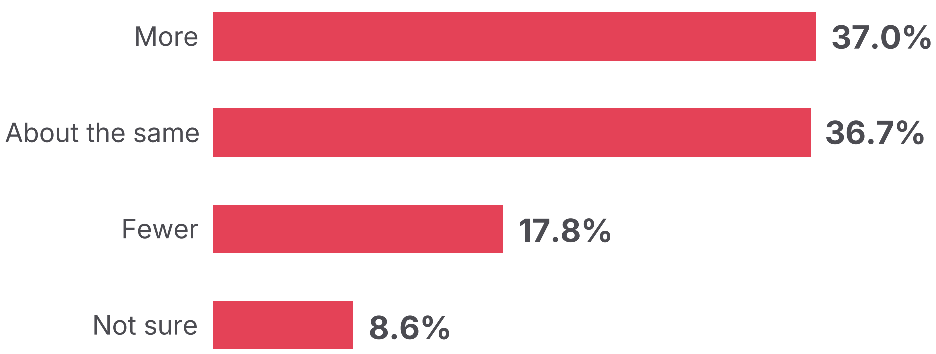
CHAPTER 5

The Next Horizon: Usage, Intent & AI

Looking Ahead to a More Intelligent Home

The smart home market is not static. Consumer behavior is evolving, and the integration of Artificial Intelligence presents both the greatest opportunity and the most significant challenge for the next generation of devices.

Q22: In the next 3 years, do you expect to use more, fewer, or the same number of smart devices?

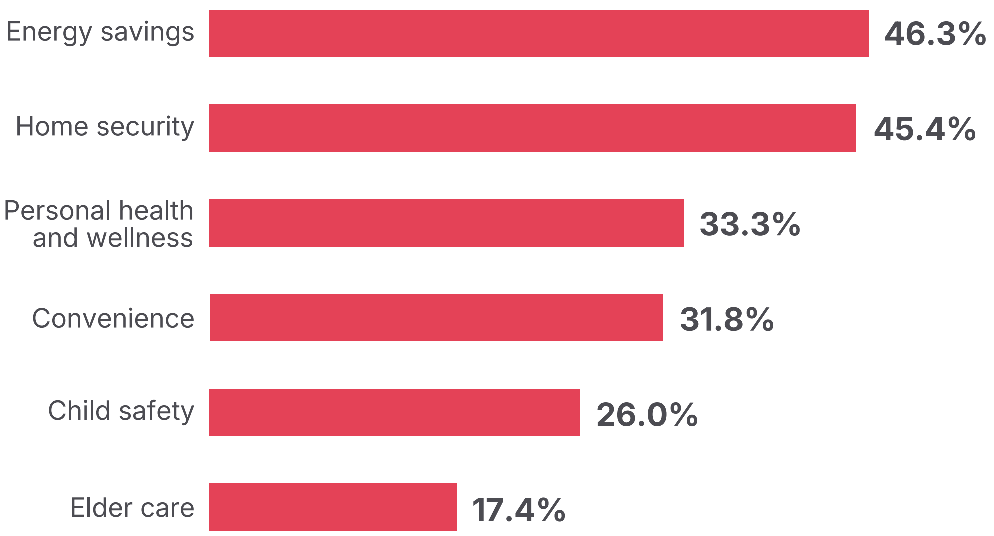


Insight: The market is poised for steady growth. The number of users expecting to increase their device count is more than double those expecting to decrease it, signaling a healthy outlook for the industry.

Q23: What would make you more likely to use (more) smart devices?

Insight: When it comes to driving further adoption, simplifying security is the number one lever. Users don't just want devices to be secure; they want to feel in control of that security in an easy, intuitive way.

Q24: What areas of life (if any) might make smart devices appealing to you in the future?

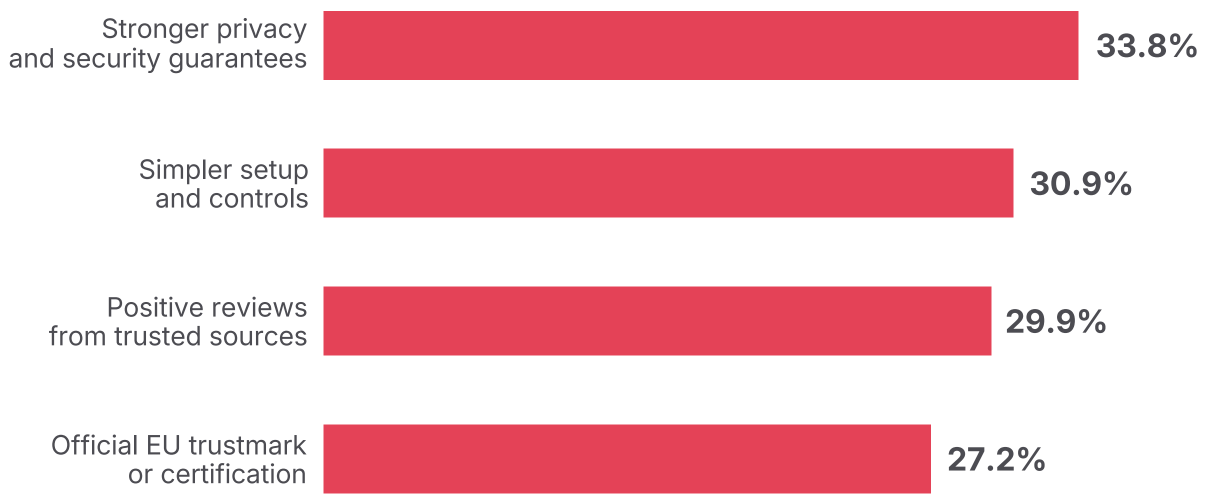


Insight: The most appealing future use cases are highly practical and centered on core human needs: saving money and feeling safe. This suggests that the market will reward products that solve tangible problems over those that offer novelty.

Connected devices already have the power to make our buildings healthier, safer, and far more energy efficient. The challenge isn't the technology, but raising awareness and showing decision makers what's possible when we put data to work.

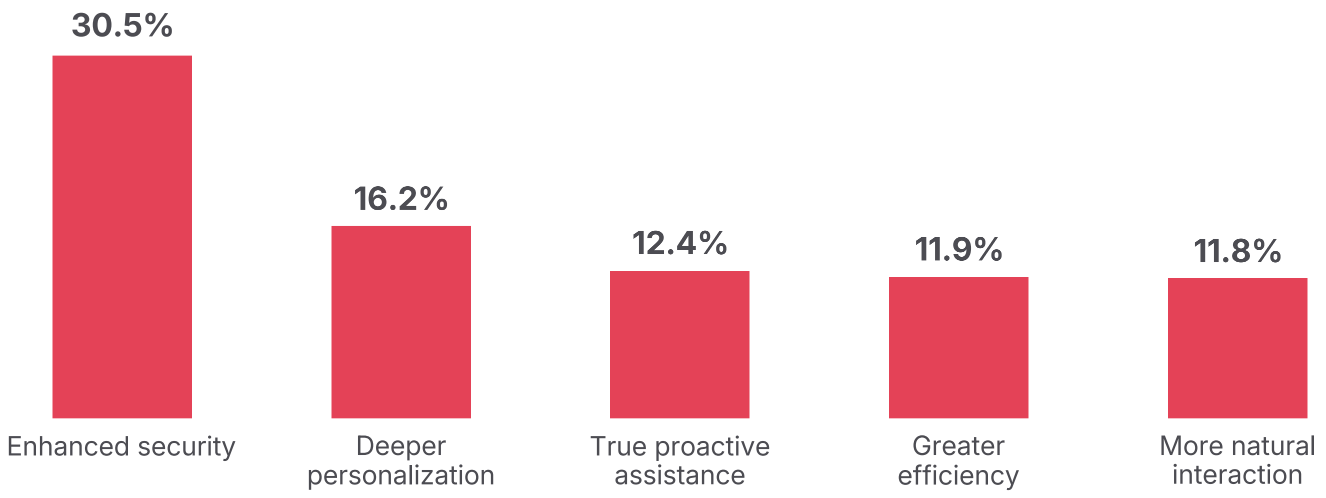
– Gaetano Lapenta, Founder & CEO, Fybra

Q25: What would make you more likely to try a smart device?



Insight: For the unconverted, the message is clear: prove it's safe, make it simple, and get a good review. This is a classic marketing challenge, but with the unique twist that "safety" (privacy guarantees) is the leading product feature.

Q26: When you think about more advanced AI being integrated into smart devices, which of these is your BIGGEST HOPE for the technology?

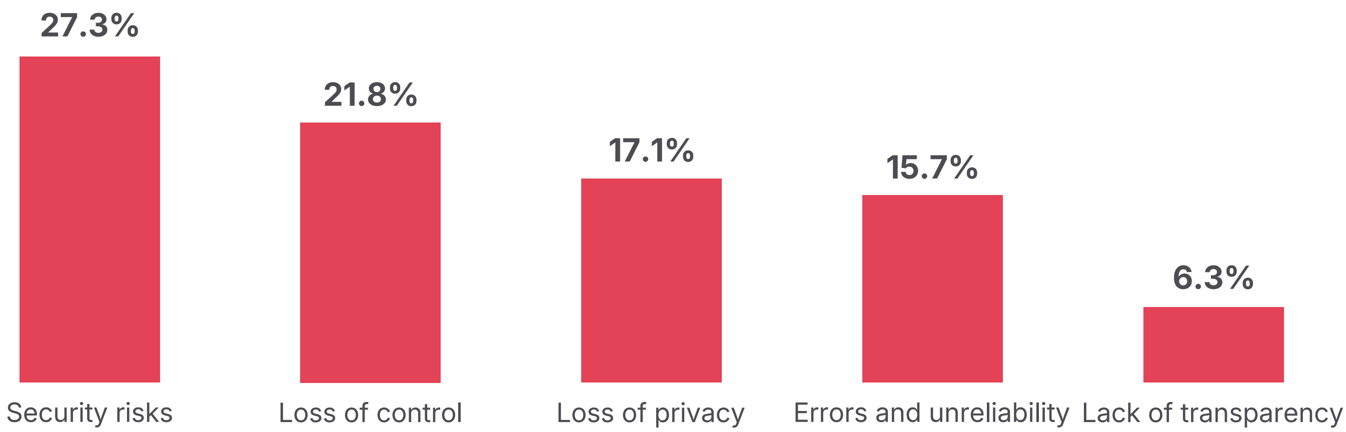


Insight: Counterintuitively, the biggest hope for AI is that it will solve the market's biggest problem: security. Consumers see intelligent monitoring as a key benefit, wanting AI to act as a digital guardian for their homes.

By running AI directly on devices, we can deliver intelligent, autonomous behavior while keeping data private and transparent. This builds trust and makes connected devices truly practical for industrial and commercial applications.

– Jon Lindén, Founder & CMO, Ekkono Solutions

Q27: And which of these is your BIGGEST CONCERN about more advanced AI in smart devices?



Insight: The greatest fear mirrors the greatest hope. Consumers worry that a more intelligent system is also a more vulnerable one, susceptible to new and more sophisticated forms of hacking. This highlights the central paradox for AI in the home: it must be powerful enough to protect us, but not so powerful that it becomes a threat itself.

Conversational AI is changing the game. Users can now get instant answers, which challenges our platform's value. To stay relevant, we need to adapt quickly and integrate with these emerging tools.

– Anand Narasipuram, Co-founder, Smartivate

Conclusions & Strategic Takeaways

The survey confirms a clear reality: adoption of IoT in Europe is driven by trust, simplicity, and usefulness. Consumers want devices that are secure, easy to use, and add real value to daily life.

For product teams, this means the winning formula is not more features, but clearer trust signals, seamless interoperability, and business models that sustain growth.

And for Europe, this is a moment of opportunity. By combining its strengths in safety, usefulness, and sustainability, Europe can set the global standard for connected living.

The task ahead is not easy, but it is clear. The companies that align with these values will define the next decade of IoT.

Europe has a unique opportunity to lead the global IoT market by combining safety, usefulness, and sustainability. This research makes it clear: trust isn't just a regulatory checkbox—it's the growth unlocker. Our mission is to help IoT startups and scale-ups design products that people not only buy, but actually trust and keep using.

– Gabriel Dombri, Salt & Pepper Partner

The Trust Blueprint:
4 Rules for Winning the European Smart Home

1. Sell Trust, Not Just Tech.

Your biggest competitor isn't another device; it's consumer inertia fueled by distrust. Lead with your privacy and security credentials. Make them visible, understandable, and central to your brand identity.

2. Embrace Regulation as a Feature.

The "EU Certified" trustmark is a powerful, consumer-requested differentiator. Proactively align with the principles of the Cyber Resilience Act and AI Act and market your compliance as a core benefit that justifies consumer confidence.

3. Solve the Seamlessness Problem.

The next unicorn in this space won't be the one with the most features, but the one that makes everything "just work" together. Invest in open standards and prioritize a frictionless user experience over a locked ecosystem.

4. Build Responsible AI.

Deliver proactive assistance, but always leave the user in control. AI that feels like a "black box" will amplify fears. AI that is transparent, explainable, and focused on tangible benefits like security and energy savings will build confidence and drive the next wave of adoption.

salt& pepper

Methodology

The insights presented in this report are derived from a comprehensive quantitative survey designed to capture a representative snapshot of smart device adoption, user sentiment, and key barriers to market growth in Europe.

Survey Instrument & Distribution

The survey was conducted via an online survey platform. The instrument consisted of 27 questions, including multiple-choice, multiple-select, and ranking questions, designed to explore consumer habits, frustrations, security perceptions, and future intentions related to IoT and smart home devices.

Data Collection Period

Data was collected in June 2025.

Sampling & Geographic Scope

The survey targeted a total of 1,200 adult consumers (aged 18+) distributed across four key European markets:

- The United Kingdom
- Germany
- The Netherlands
- Denmark

To ensure a high degree of accuracy, the sample was balanced across key demographic segments, and the final data was weighted to accurately reflect the adult population of each country. This provides a robust and representative foundation for the report's findings.

About Salt & Pepper

Salt & Pepper, the European product partner for IoT innovators, works with startups and scale-ups to design, build, and launch connected products that earn trust and scale. We combine deep technical know-how with strong product expertise and a clear, outcome-focused process.

Our approach is rooted in a core belief: the best technology is human-centric, intuitive, and, above all, trustworthy. We combine deep tech expertise with a transparent, outcome-focused process to create complex IoT ecosystems and smart devices that people love and businesses rely on.

This report, "The IoT Trust Deficit," is part of our commitment to shaping a more secure and human-centric connected future. We believe that by understanding the deep-seated needs of consumers, we can, together, build an IoT landscape that is not only innovative, but earns the trust it requires to thrive.

Ready to build the future of connected living?

LET'S TALK.

Website

Press contact: Gabriel Dombri, gabriel@saltandpepper.co