# Smart homes evolve with AI and Cyber Resilience Act to enhance security and integration



The transformation of home living through advanced technologies has led to an era of smart homes that increasingly rely on artificial intelligence (AI) and the Internet of Things (IoT). The burgeoning capabilities of these technologies are shaping a new kind of residential experience, characterised by sophisticated automation, improved connectivity, and enhanced user interaction. As AI systems become more adept at learning and anticipating individuals' needs, the integration of various smart devices fosters an environment where everything is interconnected, making daily tasks far simpler and more efficient.

Artificial intelligence is at the core of this evolution, capable not only of understanding user preferences but also of interacting in a more natural and responsive manner. Modern voice-controlled systems exhibit a level of empathy, able to recognise not just commands but also contextual nuances such as the speaker’s identity and environmental factors. Innovations in spatial hearing, environmental modelling, and on-device processing enable devices to respond with greater accuracy and speed, reducing reliance on cloud-based data processing. This technological leap allows for the creation of a cohesive smart home ecosystem, appealing to consumers' desire for integrated solutions rather than a disjointed array of devices.

According to industry forecasts, the smart home market in Europe is projected to grow from $22.1 billion in 2024 to nearly $30 billion by 2029. Central to this growth is the push for interoperability among smart devices, offering a more seamless user experience. Consumers increasingly demand a unified ecosystem that facilitates functionality without the cumbersome need for multiple apps or platforms. Products such as AI-driven security cameras, smart locks, and energy management systems are seeing significant uptake, showcasing the shift toward home security and energy efficiency.

The integration of smart home technology with other platforms, including smart grids and wearable devices, further enhances this ecosystem. Sameer Sharma, AVP of the IoT Business Unit at MediaTek, described this integration as the "holy grail" in smart home technology. Speaking to the evolving standards, he highlighted the importance of Matter, a new interoperability standard, suggesting it represents a crucial step towards unifying the myriad technologies that consumers encounter. While some competing standards may complicate purchasing decisions, Sharma notes that the consumer drive for differentiation remains strong, complicating the landscape yet further.

At the same time, significant advancements in personalisation are expected to redefine user experiences in smart homes. Imagining a future where homes learn and adapt to lifestyles — from adjusting lighting to suit evening routines to planning workouts based on past activities — presents an intriguing vision. MediaTek envisions a future where smart homes seamlessly integrate into the daily lives of residents, essentially functioning in the background to enhance convenience and comfort.

Yet amidst these advancements, cybersecurity remains a pressing concern. An estimated 80% of IoT devices are vulnerable to cyber threats, including data theft and identity fraud, exacerbated by the highly interconnected nature of these devices. Actors can exploit weaknesses in any connected device to gain broader access to a home's network, potentially leading to severe ramifications. The introduction of the EU's Cyber Resilience Act will enforce stricter cybersecurity requirements across the digital product spectrum, including connected home devices, in a bid to secure communities against the evolving threat landscape.

The Cyber Resilience Act aims to establish comprehensive standards for the design and maintenance of hardware and software products, thus safeguarding both businesses and consumers. By mandating robust security protocols throughout a product’s lifecycle, the Act intends to close the numerous gaps that currently exist in cybersecurity frameworks. With compliance deadlines set for December 2027, firms are being urged to re-evaluate their security strategies, with those failing to comply risking significant competitive disadvantage.

Looking ahead, the rapid adoption of technologies such as machine learning and generative AI will continue to reshape the smart home landscape. These innovations will work quietly in the background, anticipating needs and refining user experiences, all while mitigating the risks associated with increased digitisation. The challenge, however, remains in balancing innovation with security—a complex task in a rapidly evolving market characterised by fierce competition and continuous technological advancement. As these changes unfold, the promise of a smarter living experience is becoming an undeniable reality, even if it demands vigilance against the accompanying risks.

## Reference Map:

* Paragraph 1 – [[1]](https://www.newelectronics.co.uk/content/features/smart-living-made-simple), [[2]](https://time.com/5634791/smart-homes-future/)
* Paragraph 2 – [[1]](https://www.newelectronics.co.uk/content/features/smart-living-made-simple), [[5]](https://www.isc2.org/Insights/2024/12/Understanding-the-European-Cyber-Resilience-Act)
* Paragraph 3 – [[1]](https://www.newelectronics.co.uk/content/features/smart-living-made-simple), [[3]](https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/), [[4]](https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act)
* Paragraph 4 – [[1]](https://www.newelectronics.co.uk/content/features/smart-living-made-simple), [[6]](https://www.mofo.com/resources/insights/240523-eu-cyber-resilience-act-raises)
* Paragraph 5 – [[1]](https://www.newelectronics.co.uk/content/features/smart-living-made-simple), [[3]](https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/)
* Paragraph 6 – [[1]](https://www.newelectronics.co.uk/content/features/smart-living-made-simple), [[6]](https://www.mofo.com/resources/insights/240523-eu-cyber-resilience-act-raises)
* Paragraph 7 – [[1]](https://www.newelectronics.co.uk/content/features/smart-living-made-simple), [[2]](https://time.com/5634791/smart-homes-future/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.newelectronics.co.uk/content/features/smart-living-made-simple> - Please view link - unable to able to access data
2. <https://time.com/5634791/smart-homes-future/> - This article explores the future of smart homes, highlighting advancements in artificial intelligence (AI) and the Internet of Things (IoT). It discusses how AI will enable homes to anticipate occupants' needs, adapt schedules, and make health-related decisions. The expansion of IoT devices is expected to lead to homes that learn and adapt to their residents' preferences. The piece also addresses the importance of cybersecurity as smart homes collect and analyse personal data, emphasising the need for robust security measures to protect sensitive information from potential cyber threats.
3. <https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/> - The European Union's Council adopted the Cyber Resilience Act, establishing new cybersecurity requirements for products with digital elements, including connected home devices. The regulation aims to ensure that such products are secure before entering the market, addressing gaps and clarifying existing cybersecurity frameworks. It introduces EU-wide standards for the design, development, production, and availability of hardware and software products, ensuring security throughout the supply chain and product lifecycle. The Act applies to all products connected directly or indirectly to another device or network, with certain exceptions.
4. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act> - The Cyber Resilience Act enhances cybersecurity standards for products containing digital components, requiring manufacturers and retailers to ensure security throughout the product lifecycle. Applicable to all products connected directly or indirectly to another device or network, the Act introduces mandatory cybersecurity requirements for the design, development, production, and maintenance of such products. It aims to safeguard consumers and businesses by addressing inadequate cybersecurity levels and the lack of timely security updates. The regulation entered into force on 10 December 2024, with main obligations applying from 11 December 2027.
5. <https://www.isc2.org/Insights/2024/12/Understanding-the-European-Cyber-Resilience-Act> - This article provides an overview of the European Cyber Resilience Act (CRA), detailing its scope and implications. The CRA applies to a broad range of products with digital elements, including computers, smartphones, routers, sensors, cameras, and various smart devices. It also covers device firmware, operating systems, mobile and desktop software, software libraries, and app stores. The Act introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the planning, design, development, and maintenance of such products. It aims to enhance the digital landscape by promoting secure development practices and fostering a more resilient digital ecosystem.
6. <https://www.mofo.com/resources/insights/240523-eu-cyber-resilience-act-raises> - This article discusses the European Cyber Resilience Act (CRA) and its impact on digital products. The CRA sets minimum cybersecurity standards for hardware and software products with digital elements, aiming to ensure secure design, development, and post-market management. It introduces conformity requirements, including the need for manufacturers and developers to obtain an EU declaration of conformity and affix the 'CE' conformity mark to products. The Act also mandates vulnerability handling requirements, such as providing customers with a support period of at least five years to address vulnerabilities, unless the product's lifetime is shorter.
7. <https://www.hunton.com/privacy-and-information-security-law/cyber-resilience-act-published-in-the-official-journal-of-the-eu> - This article reports on the publication of the Cyber Resilience Act in the Official Journal of the EU. The Act regulates cybersecurity issues in the design, development, production, manufacturing, and availability of hardware and software products connected to another device or network, such as connected home cameras, fridges, TVs, toys, and other IoT products. As an EU regulation, the Cyber Resilience Act applies directly in all EU Member States. The majority of its provisions will apply from December 11, 2027, with some exceptions becoming applicable on September 11, 2026, including rules on incident reporting.