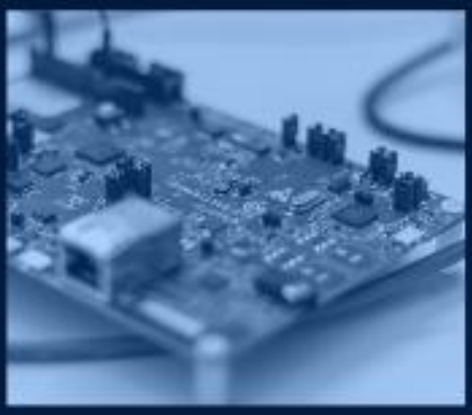
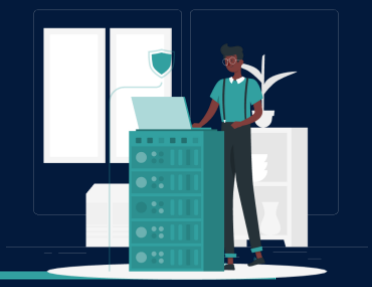
Cyber Resilience Act

How this will impact smart & connected devices


Vention Technologies B.V.
High Tech Campus 27
Eindhoven
The Netherlands
Nethe

www.vention.nl
info@vention.nl
+31 40 369 0052



Whitepaper

Table of Contents

Who is this for

This whitepaper is written for OEM's that have connected products on the market, or that are planning to bring a new connected product to the European market.
In practice, this includes many companies active in energy, healthcare, industry, agriculture, mobility, infrastructure, leisure and smart building applications.

> The Cyber Resilience Act is especially relevant for companies that place products with digital elements on the EU market. This includes products that can connect directly or indirectly to another device or network.

For many organisations, this means that a product which used to be seen mainly as a physical device is now also treated as a cybersecurity-relevant digital product.

Who should read this whitepaper?

This whitepaper is written for all stakeholders involved in delivering Product Service combinations to the market or are planning to develop and deploy new ones.

For who	Main message
Leadership teams	Cybersecurity and lifecycle support have become management responsibilities, not only engineering responsibilities.
Product and R&D teams	CRA affects product architecture, implementation, validation and documentation.
Quality and compliance teams	Evidence, risk assessment and technical documentation must be built during development instead of reconstructed at the end.
Service and operations teams	Updateability, monitoring, vulnerability handling and long-term support become part of the product lifecycle.
Companies with existing connected products	Products already in the field may need updates, documentation improvements or lifecycle process changes.
Companies developing new connected products	CRA readiness can be designed in from day one, reducing redesign risk and improving market readiness.

This whitepaper is not only for companies that already identify themselves as IoT companies. It is for every company whose products are becoming smarter, connected, more software-driven or more service-oriented.

The whitepaper is also relevant for companies that are not sure whether CRA applies to their products. Many organisations underestimate the scope because they think only obvious IoT products are affected. In reality many products with embedded software, communication interfaces or remote data processing may fall within the scope. Even when a product is not directly connected to the internet, an indirect connection to another device or network can still be relevant.

The goal of this whitepaper is not to provide legal advice. The goal is to help companies understand the practical product development impact of CRA and start the right internal discussions early on.

About Vention

With 30 engineers based at the High Tech Campus in Eindhoven, at the heart of the Brainport region, we develop, produce and support smart, scalable and future ready devices that are used across the globe. Leading companies in the energy, healthcare and industrial sector partner with us.

We bring secure, smart & connected devices to the market

We make sure that our clients are able to stay focused on their core business while relying on us to handle the complexity of developing, producing and maintaining their devices. As there is an increased need to keep devices cyber resilient, the added value of our Wockel® platform is recognised.

With our deeply embedded expertise and our approach, secured in our certified Quality Management System, we are guiding our clients from initial idea to making impact with their product.

Executive summary

The Cyber Resilience Act changes the baseline for connected products in Europe. Connected products are no longer judged only on their functional performance, cost, design and time to market. They are also rated on their ability to remain secure, updateable, supportable and transparent during their expected lifetime.

> CRA compliance cannot be fixed at the end of development. It must be designed into the product and secured within the organisation.

For companies that sell connected products as part of their service offering, this is a major shift. Cybersecurity becomes part of the product requirements, the development process, the technical documentation, the conformity assessment and the lifecycle support model. A product that works today, but cannot be securely updated or properly supported tomorrow, will become a business risk.

The CRA was introduced to address a clear problem in the market. Many digital products are placed on the market with insufficient cybersecurity. In many cases, users and customers do not know how secure a product is, how long it will be supported, whether vulnerabilities will be fixed, or how updates will be provided. As products become connected, these weaknesses affect not only one device, but also users, companies, networks, data and wider society.

What changes?

From	To
Product works at launch	Product remains secure and supportable during its expected lifetime
Cybersecurity as technical best practice	Cybersecurity as market access requirement
Documentation at the end	Evidence built during development
One-time product release	Lifecycle responsibility with updates and vulnerability handling
Device-focused view	Product, software, cloud, production and support process view
Ad hoc security response	Structured vulnerability and incident handling

The CRA introduces horizontal cybersecurity requirements for products with digital elements. This means that the regulation is not limited to one product category or one sector. It applies broadly to hardware and software products that include digital elements and that have a direct or indirect connection to another device or network.

Important dates

- **11 September 2026** Reporting obligation
- **11 December 2027** All other obligations

The main obligations will apply from 11 December 2027. Reporting obligations for actively exploited vulnerabilities and severe incidents will apply from 11 September 2026. These dates may seem far away, but for product development they are close. Connected product development often takes years. Architecture choices, hardware selection, firmware design, connectivity strategy, update mechanisms, cloud interfaces, production provisioning and service processes are decided early. If these decisions do not support CRA readiness, changes later in the project can become expensive and time-consuming or unfeasible if they concern hardware.

How are companies impacted

The CRA impacts companies in two fundamental ways. First, it changes how connected products must be developed and maintained. Cybersecurity, updateability, vulnerability handling and lifecycle support can no longer be added at the end of development. For new products, CRA readiness must be included from the first architecture, hardware, firmware, cloud and documentation decisions. For existing products, companies need to assess whether products can receive secure updates, whether software components and interfaces are known, and whether cybersecurity choices can be properly documented.

Because CRA affects product strategy, market access, lifecycle support, vulnerability handling and incident response, company officers need to ensure that responsibilities, resources and processes are properly organised.

Second, companies need to move from one-time product delivery to continuous product support. A connected product is not finished when it leaves production. It remains active in the field and must be monitored, updated and supported during its lifecycle. This requires clear ownership, processes for vulnerability response, user communication, incident handling and end-of-support decisions. Companies that prepare early can turn this into an advantage: better products, stronger customer trust and a more scalable connected product strategy.

What is the CRA and why does it matter?

The Cyber Resilience Act, or CRA, is European legislation that introduces cybersecurity requirements for products with digital elements. In practical terms, this includes many connected products, embedded devices, IoT devices, software products and hardware products that can communicate directly or indirectly with another device or network.

Why was CRA created?

Market development	Resulting cybersecurity risk
Products are increasingly connected	Vulnerabilities affect devices, users, networks and other systems.
Physical products now include software and data flows	Security depends on firmware, cloud services, apps, APIs and update processes.
Products remain in use for many years	Vulnerabilities discovered after launch must still be managed.
Users cannot always judge product security	There is limited transparency about updates, support and vulnerability handling.
Digital products are used in business and critical operations	Product security affect continuity, safety, data and trust.

The CRA was created because digital products have become part of daily life, business operations and critical infrastructure. Products that used to be standalone are now connected to apps, cloud platforms, APIs, service tools, production environments and customer systems. This creates new value, but also new cybersecurity risks.

A vulnerability in a connected product can expose data, disrupt service, affect safety, harm networks or create access points into other systems. The risk is no longer limited to the device itself. A connected product is part of a larger ecosystem.

At the same time, the market has not always provided enough transparency. Customers and users often cannot easily assess whether a product is secure, whether it receives security updates, how long it will be supported, or how vulnerabilities are handled. This creates an information gap between manufacturers and users.

The CRA addresses this by making cybersecurity a legal requirement for placing products with digital elements on the EU market. It requires manufacturers to consider cybersecurity risks during design, development, production and maintenance. It also requires manufacturers to organise vulnerability handling and provide security updates during the lifecycle of the product.

CRA changes cybersecurity from a best practice into a market access requirement.

What is the relation with RED-DA[1]

The CRA is broader than earlier product cybersecurity requirements for radio equipment.

Topic	RED-DA cybersecurity	CRA
Main focus	Radio equipment and specific cybersecurity requirements for radio products.	Products with digital elements and the related manufacturer processes.
Product view	Mainly the radio product itself.	Product lifecycle, including development, updates, documentation and vulnerability handling.
Scope of concern	Network protection, privacy and fraud protection for applicable radio equipment.	Secure design, vulnerability handling, SBOM, updates, reporting, support period and technical documentation.
Practical impact	Cybersecurity becomes part of CE marking for radio products.	Cybersecurity becomes part of product development and lifecycle responsibility for digital products.

For many companies, this is a major change. Historically, product compliance often focused on safety, EMC, radio performance and other technical requirements needed to place a product on the market. Cybersecurity was sometimes addressed as a technical design topic, but not always as a structured lifecycle obligation. CRA changes that.
A connected product must not only be sufficiently secure at launch. It must be maintainable during its support period.

[1] See our whitepaper on RED-DA: Link

This means the manufacturer must be able to identify vulnerabilities, assess their relevance, provide updates, inform users and maintain documentation.
CRA is therefore relevant for product strategy, not only for compliance. It affects how products are specified, designed, built, tested, documented, sold, supported and maintained. See also our Whitepaper on Innovation: Link

Important shift
The product is no longer finished when it leaves production. The product remains your responsibility during its lifecycle.

Why companies need to act before the final deadline

The regulation also matters because product development timelines are long. Waiting until 2027 is risky. Many architecture choices that determine CRA readiness are made much earlier. For example, if a product does not have enough memory for secure update mechanisms, if the hardware does not support secure key storage, if the boot chain cannot protect firmware integrity, or if the cloud architecture does not support secure device management, these issues are difficult to solve later.

The same applies to documentation and processes. A software bill of materials is much easier to maintain when it is integrated into the development workflow from the beginning. Vulnerability handling is easier when ownership, tooling and response procedures are already defined. Technical documentation is easier when design decisions, risks, interfaces and mitigations are documented as the product is developed.

For companies that act early, CRA can become more than a compliance burden. It can become a driver for better product development. A product that is secure by design, updateable, documented and supportable is also more attractive to customers. It reduces lifecycle risk and supports long-term value.

The CRA is not only a regulation. It is driving mature products that are supporting key functions.

Companies with existing products

Companies with existing connected products should not wait until the final CRA deadline before acting.

Many products that are already on the market were designed before CRA was known, or before cybersecurity was treated as a formal product lifecycle requirement. These products may work well in the field and be commercially successful, but they probably still have gaps when assessed against the expectations introduced by CRA.

Two perspectives for existing product review

Technical readiness

Can the product meet the expected cybersecurity requirements?

This includes secure communication, authentication, protection of sensitive data, secure update mechanisms, attack surface reduction, logging, resilience and secure configuration.

Organisational readiness

Can the company maintain the product securely?

This includes Software Bill Of Material (SBOM) management, vulnerability monitoring, risk assessment, incident response, user communication, documentation maintenance and support period management.

Typical gaps in existing connected products

Gap	Practical consequence
Limited updateability	Vulnerabilities are difficult and/or expensive to fix in the field.
Incomplete interface documentation	Attack surfaces and access paths may be unclear.
Unclear software component visibility	It becomes difficult to know whether new Common Vulnerabilities and Exposures (CVEs) affect the product.
Insufficient vulnerability monitoring	Security issues may be found too late or handled reactively.
Weak lifecycle ownership	No clear owner for security decisions after launch.
Outdated cryptographic choices	Technical security may no longer match state-of-the-art expectations.
Undocumented security assumptions	It becomes difficult to demonstrate why the product is sufficiently secure.
No structured product security incident response	Severe incidents may create delays, confusion and communication risk.

A common example is firmware updateability. Some connected products can be updated remotely, but the update process may not be designed specifically for security updates. Other products can only be updated locally or during service visits. Some products have no practical update mechanism at all. Under CRA, the ability to address vulnerabilities through security updates becomes a central lifecycle requirement.

Another example is software component visibility. Existing products often contain open-source libraries, third-party modules, operating systems, communication stacks and vendor SDKs. If there is no software bill of materials, it becomes difficult to know whether a newly discovered vulnerability affects the product. Without this visibility, vulnerability handling becomes slow, incomplete or reactive.

Documentation is another major challenge. For older products, design decisions may exist in different places: engineering notes, tickets, source code, test reports, supplier documents or personal knowledge. CRA expects technical documentation that explains how cybersecurity risks are addressed. Reconstructing this later takes significant effort, especially when engineers have moved on or the product has changed over time.

How is product lifecycle support organised?

For existing products lifecycle responsibilities may be unclear. Who monitors vulnerabilities? Who decides whether a vulnerability is relevant? Who approves a security update? Who informs customers? Who maintains user instructions? Who decides when a product reaches end of support? If these responsibilities are not clear, response time and decision quality suffer.

Responsibility area	Question to answer
Vulnerability monitoring	Who monitors vulnerabilities?
Vulnerability relevance	Who decides whether a vulnerability is relevant?
Security updates	Who approves a security update?
Customer communication	Who informs customers?
User information	Who maintains user instructions?
End of support	Who decides when a product reaches end of support?
Technical documentation	Who keeps evidence and documentation up to date?

This is especially relevant for companies that sell products under their own name. Under CRA, responsibility lies with the manufacturer. In practice, this means that outsourcing development or using third-party modules does not remove the need to understand and manage product cybersecurity. A company placing the product on the market must still be able to demonstrate that the product and the relevant processes meet the requirements.

For companies developing new products

For companies developing new connected products, the Cyber Resilience Act should be treated as an architecture input from day one.

This is the most efficient moment to act. Early in development, the product architecture is still flexible. Hardware choices, firmware design, connectivity strategy, cloud integration, update mechanisms, production provisioning and service processes can still be shaped. Once these choices are fixed, cybersecurity improvements become more expensive and less elegant.

CRA readiness starts with understanding that a connected product is not only the physical device.

A connected device is a software driven integrated system that may include sensors, electronics, firmware, wireless communication, apps, cloud services, APIs, production tools, provisioning flows, device management, service dashboards, data storage and user processes. Security must be considered across that system.

Connected product system view

Product layer	CRA-relevant topics
Physical product	Electronics, hardware security, debug access, memory, secure elements, labels and identifiers.
Firmware	Secure boot, firmware integrity, updateability, logging, access control and configuration.
Connectivity	Device identity, authentication, encryption, protocols and exposed interfaces.
Cloud and backend	Device management, access control, monitoring, APIs and data handling.
Apps and user interfaces	Secure access, user control, transparency and secure operation.
Production	Provisioning, keys, certificates, firmware versions, test logs and configuration data.
Service and lifecycle	Vulnerability handling, updates, support period, diagnostics and customer communication.

For new products, this means cybersecurity needs to be part of the product requirements. It is not a separate work package added at the end. Requirements must cover secure communication, authentication, access control, secure storage, firmware integrity, software updates, logging, data minimisation, attack surface reduction, resilience and secure user operation.

Early architecture decisions that matter

One of the most important design decisions is updateability. If a product cannot be updated securely, it becomes difficult to maintain during its lifecycle. Security vulnerabilities will be discovered over time, including in third-party components. The product must have a practical and secure way to receive updates. This includes firmware update mechanisms, update authentication, rollback protection, version control, testing and a controlled release process.

Another important topic is software component management. Modern embedded products often depend on operating systems, libraries, communication stacks, vendor SDKs and open-source software. For CRA readiness, companies need to know what is inside the product. This means that SBOM generation and dependency management should be integrated into the development workflow from the start.

Hardware choices also matter. Cybersecurity requirements can influence memory size, processor selection, secure element usage, key storage, debug access, boot architecture and over-the-air update strategy. A decision that looks cheaper in the prototype phase can become expensive if it limits security functionality later.

Cloud and backend choices are equally important. Many connected products rely on device management, remote configuration, data processing or service tools. The security of these interfaces matters because they can become attack paths. Access control, device identity, encryption, logging, monitoring and operational procedures must be designed as part of the product ecosystem.

Production must also be included. Secure products need secure provisioning. Device identities, keys, certificates, firmware versions, test logs and configuration data must be handled in a controlled way. If production processes are not designed securely, a well-designed product can still be weakened before it reaches the customer.

In short

- **Updateability**
  Determines whether vulnerabilities can be fixed during the support period.
- **Hardware platform**
  Determines whether secure storage, memory and security features are available.
- **Firmware architecture**
  Determines whether secure boot, integrity protection and update mechanisms are possible.
- **Device identity**
  Determines whether devices can be authenticated and managed securely.
- **Cloud architecture**
  Determines whether remote access, device management and monitoring are controlled.
- **Production provisioning**
  Determines whether keys, certificates and firmware are handled securely.
- **SBOM and dependency management**
  Determines whether software components can be monitored for vulnerabilities.
- **Technical documentation**
  Determines whether cybersecurity decisions can be proven later.

Documentation should be built during development

For new products, technical documentation should be built during development. This is more efficient than reconstructing it later. The documentation should explain the intended use, foreseeable use, cybersecurity risks, assets, interfaces, components, security mechanisms, test evidence and user instructions. Good documentation is not separate from engineering. It is the structured output of good engineering.

This requires an integrated way of working. Product management, electronics, embedded software, cloud development, compliance, quality, production and service should work from the same product assumptions. Cybersecurity decisions should be made explicitly and documented.

Practical CRA readiness checklists

Product readiness

	Checks to be executed
☐	Does the product include digital elements, and can it connect directly or indirectly to another device or network?
☐	Is the intended and reasonably foreseeable use of the product clearly defined?
☐	Has a cybersecurity risk assessment been performed and documented for the product?
☐	Are cybersecurity requirements included in the product architecture and design decisions?
☐	Is the product delivered in a secure default configuration?
☐	Can the product receive security updates during the support period?
☐	Are firmware and software updates authenticated and protected against manipulation?
☐	Does the product have a secure and controlled device identity mechanism?
☐	Are access paths protected with appropriate authentication and access control?
☐	Are relevant communication channels protected with state-of-the-art security mechanisms?
☐	Are keys, credentials, configuration and sensitive data stored securely?
☐	Are exposed interfaces, ports, services and debug access limited and documented?
☐	Does the product provide relevant security logging or diagnostic information?
☐	Is there a software bill of materials or reliable overview of software components and dependencies?
☐	Are known vulnerabilities in product components identified, assessed and mitigated where relevant?
☐	Can users securely remove data and settings where applicable?
☐	Are secure installation, operation, update and maintenance instructions provided?
☐	Is there test evidence showing that the security mechanisms work as intended?

vention

Organisational readiness

	Question to answer
☐	Is it clear who is the manufacturer and who carries CRA responsibility for the product?
☐	Is there an owner for product cybersecurity after market introduction?
☐	Has the product support period been defined and communicated?
☐	Is there a process to monitor vulnerabilities in product software, hardware and third-party components?
☐	Is there a process to decide whether a vulnerability is applicable, exploitable, mitigated, accepted or fixed?
☐	Is there a clear process and contact point for external vulnerability reports?
☐	Is there a controlled process to develop, test, approve and release security updates?
☐	Is there a product security incident response process for severe incidents and actively exploited vulnerabilities?
☐	Is it clear who reports relevant vulnerabilities or incidents to the required authorities and within which timelines?
☐	Is there a process to inform users about security updates, incidents, mitigation actions and end of support?
☐	Is SBOM creation and maintenance integrated into the development and release process?
☐	Are suppliers, third-party components and open-source dependencies assessed for cybersecurity impact?
☐	Is technical documentation kept up to date during the support period?
☐	Are cybersecurity requirements included in the product development process and design reviews?
☐	Are security requirements included in verification, validation and regression testing?
☐	Is there a process for update, redesign, phase-out and end-of-support decisions?
☐	Are responsibilities between product management, R&D, quality, compliance, service and operations clear?
☐	Is product cybersecurity periodically reviewed by management as part of lifecycle governance?

Conclusion

The Cyber Resilience Act changes the way companies need to look at connected products. Cybersecurity is no longer a technical topic that can be added at the end of the development process, but becomes a structural part of product strategy, architecture, documentation and lifecycle support. For existing products, this means companies need to assess in time whether their products are updateable, properly documented and secure to maintain. For new products, it means CRA readiness must be included from the first design decisions.

Companies that start early can use the CRA as an opportunity to develop better, safer and more future-ready products. By integrating cybersecurity by design, secure updates, vulnerability management and lifecycle support from the start, compliance becomes more achievable and customer trust increases. In this way, cyber resilience is not only a regulatory obligation, but a distinguishing element of professional connected product development.

How Vention can help

Capability	Description
CRA impact assessment	Identify which products are likely affected and where the main technical and organisational gaps are.
Cybersecurity by design	Include security requirements in product architecture, implementation and verification from the start.
Secure connected product development	Develop secure by design cloud connected devices with secure communication, device identity and updateability.
Migration services	Wockel can be deployed on most ARM platforms and delivers a secure platform out of the box
Lifecycle support	Support products after launch through updates, diagnostics, monitoring and controlled improvement.
Compliance support	Connect product development choices to CE, RED-DA, CRA and related documentation needs.
Wockel® modular platform	Provide a reusable foundation for secure, connected and updateable products, reducing the need to rebuild generic functionality.

The added value of Vention is that these capabilities are not treated as separate workstreams. In connected product development, choices in hardware, firmware, cloud, production and service are strongly connected. A decision in one area can affect security, compliance, cost, manufacturability and lifecycle support in another. Vention brings these disciplines together, helping companies make the right choices early.

Vention's Wockel® modular platform further accelerates CRA-ready product development. It provides reusable building blocks for secure connectivity, device management, firmware updates, provisioning and lifecycle support. This allows companies to focus more on the distinctive functionality of their product, while relying on a proven foundation for the generic but critical connected product capabilities.
In short, Vention helps companies move from uncertainty to a practical roadmap: what needs to be assessed, what needs to be improved, what can be reused and what should be designed into the product from day one. This makes CRA readiness more manageable and helps companies bring secure, future-ready connected products to market with more confidence.

Wockel®

Wockel® is Vention's **modular platform** that forms the basis for low-power, smart and connected **devices**. It combines reusable electronics, embedded software and (private) cloud integration. It provides robust building blocks for connectivity, cybersecurity, provisioning, device management, firmware updates, data processing, cloud integration and other user interfaces.

The platform is based on **Zephyr RTOS**, combined with reusable electronics and (private) cloud integration based on LWM2M. The Wockel platform is used on many devices in multiple industries for specific applications. All benefitting from the robustness and build-in security of the platform.

Wockel® also enables **RED-DA compliance and CRA readiness**. For wireless connected products, this means that cybersecurity, secure communication, privacy-related design choices, updateability, documentation and verification evidence are considered early in the architecture, instead of being treated as late-stage certification topics. The EU Radio Equipment Directive (RED-DA) provides the regulatory framework for radio equipment and includes essential requirements such as safety, EMC and efficient use of spectrum, with additional aspects such as privacy, personal data and fraud protection; the Cyber Resilience Act (CRA) introduces cybersecurity requirements for products with digital elements across design, development, production and expected use.

Wockel® can be **applied in different ways** depending on the situation:

1. As foundation for a completely new to be developed connected product
2. As migration path for existing products running on ARM-based hardware
3. As basis for a custom communication PCBA that adds secure connectivity and device management to a new or existing product.

This makes Wockel® suitable both for new product development and for modernising existing products that need to become smart, connected, updateable and lifecycle ready.

See more info on website: Link