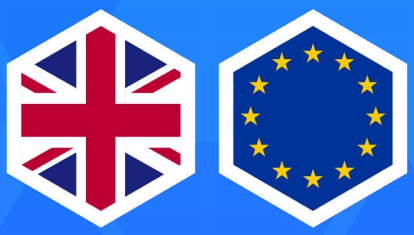
sonatype

Meet CRA Compliance Requirements with Sonatype

A User's Guide to
Cyber Resilience Act (CRA) Compliance



The EU Cyber Resilience Act (CRA)

The CRA has been developed to improve the cybersecurity of digital products by establishing essential requirements for manufacturers to ensure their products reach the market with fewer vulnerabilities. The CRA is expected to be **formally adopted later in 2024**, with most of its provisions becoming enforceable in 2027. **It applies to any software or hardware product** and its remote data processing solutions, as well as products with digital elements whose intended use includes a logical or physical data connection to a device or network.

The CRA is expected to be formally adopted later in 2024, with most of its provisions becoming enforceable in 2027.

The CRA seeks to strengthen the detection and response to cybersecurity incidents by:

Raising the overall level of cybersecurity across the EU

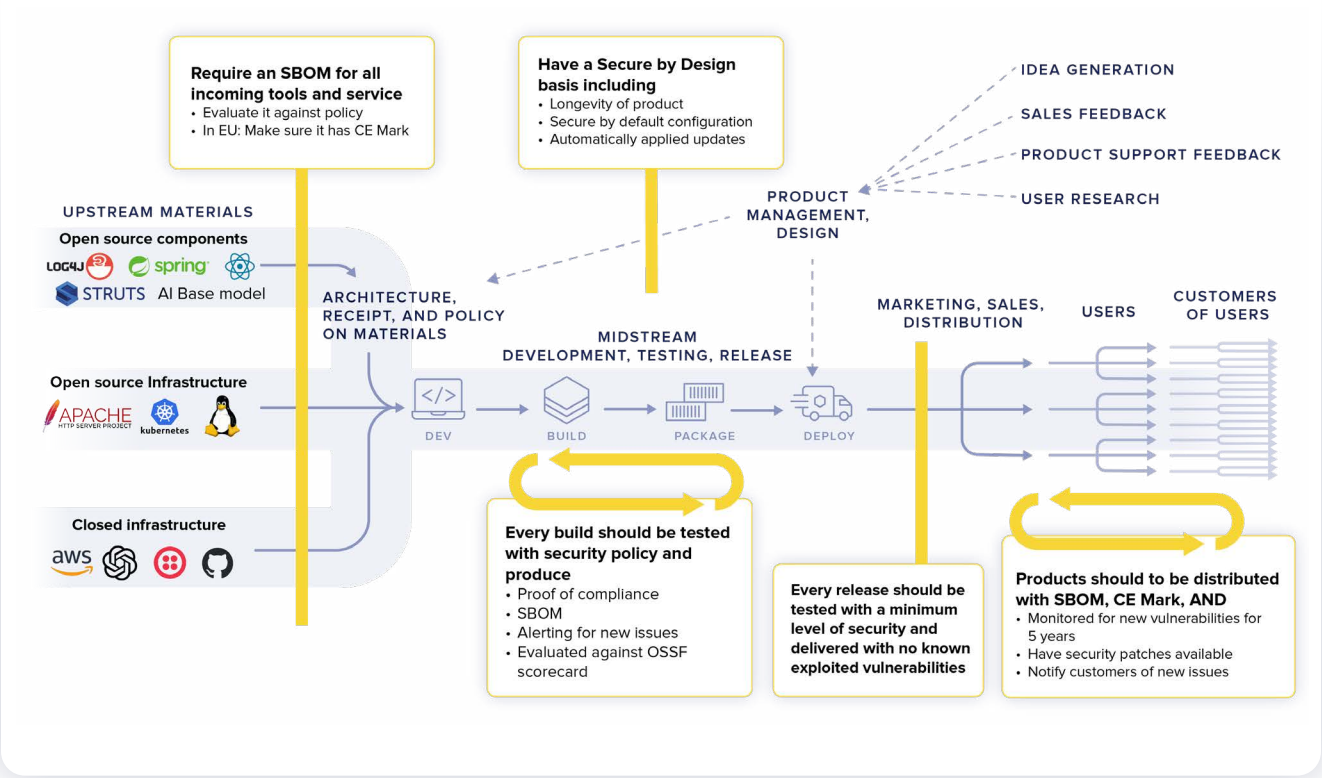
Requiring all software components to obtain the CE mark

Holding organisations liable if found to be non-compliant

The **European Commission** issued eight annexes to supplement the CRA, the first of which deals exclusively with **Essential Cybersecurity Requirements**. Manufacturers can only introduce products to the market that comply with the requirements of Annex I.

These requirements are divided into two categories: **Information Security** and **Vulnerability Management**, and here we outline how the Sonatype platform helps meet these requirements.

Like most emerging cybersecurity legislation, the CRA has been developed wit an eye toward protecting open source software. Incorporating robust security measures into the development process is necessary to strengthen your approach OSS components and SDLC processes that take into account established best practices will minimize risks.



ANNEX I, ARTICLE 1:

Security Requirements Relating To The Properties Of Products With Digital Elements

Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks	The minimum requirement for vulnerability management according to ENISA and several national CERTs is to be able to produce and monitor software bills of material for all software. **The Sonatype platform allows you to do that for all of your software built and purchased as well as the open source and third-party components encapsulated within them**
Products with digital elements shall be delivered without any known exploitable vulnerabilities;	Delivering without KEVs cannot be done without some level of certification. **The Sonatype platform** keeps track of all known security vulnerabilities with the industry's best knowledge base, and updates you about any new discoveries with automatic remediation action. **Our context- and process-aware policy allows you to control what is allowed to be released in an incremental, proactive fashion, ensuring all software is clean as it is released.**
On the basis of the risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: **a.** be made available on the market without known exploitable vulnerabilities; **b.** be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor made product with digital elements, including the possibility to reset the product to its original state; **c.** ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate time-frame enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;	More than 90% of all code in software is third-party or open source in origin. **Sonatype's SCA platform allows you to identify, monitor, categorise, and affect these third-party dependencies.** Our uniquely architected platform is designed to generate SBOMs that identify the name, version, purpose, known risks, and known licences of these third-party components, allowing you to be fully aware of the potential attack surface, and intended use case of the components.

d. ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

e. protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

f. protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

g. process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (minimisation of data);

h. protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

i. minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

j. be designed, developed and produced to limit attack surfaces, including external interfaces;

k. be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

l. provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

m. provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Once you have awareness, you can begin to make better architectural decisions. **The Sonatype platform** supports this by giving you enterprise-grade reporting on the technology base you are using, component overlap, and the most critical components and risk.

ANNEX I, ARTICLE 2:

Vulnerability Handling Requirements

1. Identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;	**The Sonatype platform allows you to identify known vulnerabilities and documents in third-party components.** It also generates a standards-compliant, machine-readable CycloneDX or SPDX SBOM which is automatically updated as the software continues to be built as a part of the standard SDLC / DevOps pipeline of an organisation.
2. In relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;	**The Sonatype platform** provides automatic remediation suggestions for any known vulnerability, including transitive dependencies. Our advanced remediation engine allows collecting remediation into golden PRs, which minimises the work needed to address vulnerabilities. **Our industry leading vulnerability intelligence gives clear, concise descriptions of what the affected code is, allowing for fast action.**
3. Apply effective and regular tests and reviews of the security of the product with digital elements;	**The Sonatype platform** is designed to run on a continuous basis in our customer's SDLC and Devops pipelines. This means our testing can be performed as often as a build is performed with the help of over 30 out-of-the-box integrations that can be used to increase coverage and frequency.
4. Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;	**Sonatype's industry leading OSS** Knowledge Base contains detailed vulnerability intelligence about open source vulnerabilities, including fixed versions, descriptions, affected components and code, as well as a host of useful remediation advice.

5. Put in place and enforce a policy on coordinated vulnerability disclosure;	**The Sonatype platform** can ingest any disclosed vulnerability contained within a software's SBOM.
6. Take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	**The Sonatype platform** and intelligence can help facilitate communication about known and unknown components
7. provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;	**The Sonatype platform Nexus Repository** can be used as an update site, giving you the ability to distribute your software updates in a scalable fashion.

CRA Reporting Requirements

Security vulnerability reporting is, understandably, a key requirement of the CRA, and Article 11 requires software publishers to disclose unpatched vulnerabilities to government agencies within 24 hours of exploitation. Reporting obligations include:

CRA Reporting Obligations for Manufacturers

A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established in Article 16.	**Sonatype SBOM Manager generates an updated Vulnerability EXchange (VEX) file to accurately report on known security vulnerabilities in SBOMs.** This tool is essential for communicating the current status of vulnerabilities, particularly those remediated or addressed in production. Sonatype's software supply chain security platform provides comprehensive access to and reporting on the overall security posture of the supply chain.
After becoming aware of an actively exploited vulnerability or a severe incident, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, about an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements and, where necessary, about risk mitigation and any corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured and easily automatically processible machine-readable format. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.	**Sonatype SBOM Manager** generates an updated Vulnerability EXchange (VEX) file to accurately report on known security vulnerabilities in SBOMs. This tool is essential for communicating the current status of vulnerabilities, particularly those remediated or addressed in production. Sonatype's Software Supply Chain Security Platform provides comprehensive access to and reporting on the overall security posture of the supply chain.

Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements, report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Annex I, Part II.	**Sonatype SBOM Manager** generates an updated Vulnerability EXchange (VEX) file to accurately report on known security vulnerabilities in SBOMs. This tool is essential for communicating the current status of vulnerabilities, particularly those remediated or addressed in production. Sonatype's Software Supply Chain Security Platform provides comprehensive access to and reporting on the overall security posture of the supply chain.
Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format	**Sonatype SBOM Manager** generates an updated Vulnerability EXchange (VEX) file to accurately report on known security vulnerabilities in SBOMs. This tool is essential for communicating the current status of vulnerabilities, particularly those remediated or addressed in production. Sonatype's Software Supply Chain Security Platform provides comprehensive access to and reporting on the overall security posture of the supply chain.

Optimise and Protect Your Software Supply Chain

The CRA is sweeping, and because it applies to anyone publishing software, its impact will be felt across virtually every industry. Only products that comply with the security and vulnerability management requirements above will be allowed on the market. Products will be presumed to be compliant, but if they are discovered not to be, sanctions will apply.

The Sonatype platform can help developers gather and report on compliance information, identify vulnerabilities, and meet the reporting requirements of CRA. To learn more about how we can help you ensure compliance with emerging and existing regulations, schedule a demo today.

sonatype

Sonatype is the leader in software supply chain optimization. Sonatype's platform empowers enterprises to create safer software faster and to protect against the inherent risk from free open source components used to develop modern software applications. As founders of Nexus Repository and stewards of Maven Central, the largest public repository of Java, Sonatype pioneered software supply management and maintains the world's leading knowledge base of open source intelligence for software composition analysis and dependency management.

Sonatype's platform integrates this intelligence with customers' Software Development Life Cycle and delivers reliable automated identification and remediation of vulnerable and malicious open source code while also enabling customers to generate and continuously monitor SBOMs (Software Bill of Materials) to increase their security posture and be prepared for the next zero-day threat or software supply chain attack.

More than 2,000 organizations, including 70% of the Fortune 100, fifteen million software developers and hundreds of government customers rely on Sonatype to set and enforce policies for open source governance, and "shift left" to deliver software applications that are secure by design and secure by default. For more information, please visit **Sonatype.com**, or connect with us on **Facebook**, **Twitter**, or **LinkedIn**.

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High
St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place,
Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com