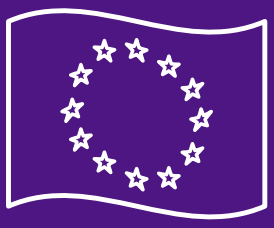
WHITE PAPER

Understanding the Cyber Resilience Act's Security Requirements for Digital Products



With the European Council's recent adoption of the Cyber Resilience Act, a new chapter in cybersecurity regulation opens, promising to reshape how digital products are developed and maintained across the EU. It aims to establish horizontal cybersecurity requirements for digital products and connected devices, ensuring these products are more secure when placed on the market and throughout their lifecycle.

The regulation is designed to address increasing cybersecurity threats from connected devices, aiming to protect both businesses and consumers. It seeks to reduce the vulnerabilities in hardware and software by introducing security standards that manufacturers must follow. This is to prevent attacks, ensure timely security updates, and provide consumers with clear cybersecurity information.

The Cyber Resilience Act was first announced by Commission President von der Leyen in September 2021 and was subsequently highlighted in the Council's conclusions on enhancing the EU's cyber posture. The proposal builds on existing frameworks like the NIS directive and the EU Cybersecurity Act, ensuring a consistent approach across different sectors. This Act reflects the EU's broader cybersecurity strategy, including the ambition to position the Union as a global leader in secure digital products.

Bridging the Cybersecurity Gap

The Cyber Resilience Act aims to address significant gaps in the current cybersecurity landscape. By introducing EU-wide requirements, the Act ensures that digital products—from smart home cameras to connected toys—are safe before they hit the market. This legislation is designed to make the existing framework more coherent and comprehensive, particularly for Internet of Things (IoT) products, safeguarding them throughout their lifecycle.

The act applies to all products with digital elements that are made available on the European Union market, including software, hardware, and connected devices. Special emphasis is given to products critical for societal and economic functions. It introduces several pivotal changes:

EU-Wide Requirements

The regulation standardizes cybersecurity requirements for the design, development, production, and market availability of both hardware and software. This harmonization seeks to prevent regulatory overlap among EU member states while simplifying compliance for manufacturers.

CE Marking

Products compliant with the regulation will bear the CE marking, a symbol of safety, health, and environmental protection standards within the European Economic Area (EEA). This marking is crucial for maintaining high-quality standards across the single market.

Scope of Application

The regulation applies broadly to all products connected to devices or networks, with some exceptions, such as medical devices and aeronautical products, which are already covered by existing EU cybersecurity rules.

Empowerment

The Act empowers consumers and businesses by making it easier to identify products with robust cybersecurity features, allowing them to make informed decisions when selecting digital products.

Key Provisions

Cybersecurity-by-design

Manufacturers must ensure their products have built-in cybersecurity measures.

Transparency for Users

Users should be informed about the support period and security features of digital products.

Regular Security Updates

Manufacturers must provide necessary security updates throughout the product's lifecycle.

Conformity Assessments

Products will be classified based on risk (important vs. critical), and high-risk products must undergo third-party cybersecurity assessments.

Role of Manufacturers, Importers, and Distributors

All stakeholders in the supply chain, including manufacturers, importers, and distributors, have responsibilities under this regulation. This includes maintaining product security during distribution and ensuring cybersecurity requirements are met for imported goods.

Exemptions and Specific Cases

Certain categories of products are exempted, such as medical devices, which already fall under existing sector-specific cybersecurity regulations. The Act also provides provisions for open-source software and non-commercial activities, focusing more on products sold in the course of a commercial activity.

Five Ways How Armis Helps

Armis applauds the Council's new law on security requirements for digital products and we believe the importance of this plan cannot be overstated. Our role is to help businesses across the world secure their environments without fear of an attack by securing every asset, from the ground to the cloud, that is being connected to the network now and in the future.

We have built a platform, Armis Centrix™, that sees every single asset type: IT, OT, IoMT, IoT, Virtual and Cloud, protecting the entire attack surface and managing cyber risk exposure in real time. Here are a ways where Armis plays a significant role in supporting organizations and manufacturers to comply with the Cyber Resilience Act (CRA):

1 Attack Surface Management

The Cyber Resilience Act emphasizes the importance of securing products with digital elements throughout their lifecycle. Armis offers visibility across all connected devices in an enterprise's network, including unmanaged and IoT devices that are often harder to monitor. Armis empowers organization to:

- Identify and inventory all digital products within their ecosystem.
- Monitor assets in real-time by continuously tracking device behavior, communication, and any potential breaches or unauthorized access.

2 Prioritization and Remediation of Security Findings

A key requirement of the CRA is ensuring regular security updates and timely vulnerability management. Armis Centrix™ is the platform of choice for manufacturers and organizations to:

- Consolidate and prioritize all security findings, including vulnerabilities and misconfigurations in connected devices and software that could be exploited.
- Automate remediation processes and ensure security updates are applied consistently, helping organizations comply with CRA's mandates around vulnerability handling.
- Monitor and track whether critical updates are missing from digital products.

3 Cybersecurity Risk Assessment

The CRA demands that manufacturers perform security risk assessments during the design, development, and maintenance phases of their products. Armis transforms this process by:

- Providing real-time risk assessments across all connected devices, allowing manufacturers and organizations to understand the risk posture of their products in dynamic environments.
- Identifying potential attack vectors and providing insights on how vulnerabilities can propagate across systems through lateral movement.

4 Compliance and Reporting

The CRA and other frameworks like Center of Internet Security Critical Security Controls (CIS Controls) and the NIST CyberSecurity Framework (CSF) require detailed information and reports about every device in your environment. Their scope includes managed, unmanaged, and IoT devices that are on your network (both wired and Wi-Fi) as well as off your network and communicating via public Wi-Fi, Bluetooth, and other peer-to-peer IoT protocols.

Unlike visibility tools that simply tell you a device's IP and MAC addresses, Armis Centrix™ gives you in-depth information about each device. This visibility is important for compliance and reporting cases. Armis Centrix™ lets organizations demonstrate compliance with the CRA by providing:

- Audit trails and reporting capabilities, which would help manufacturers and businesses document cybersecurity efforts, security updates, and vulnerability management for regulatory purposes. Armis has been designed to ensure real-time asset alignment with compliance standards and security frameworks
- Alerts and reports when non-compliant or unauthorized devices are detected on the network, helping organizations maintain compliance with the CRA's strict security requirements.

5 Support for Critical Infrastructure

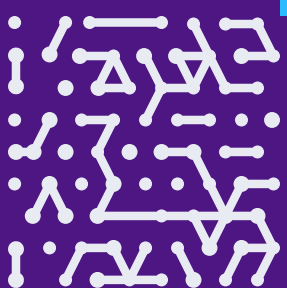
The CRA identifies "critical and important products" (such as connected healthcare devices or industrial control systems) that require stricter cybersecurity measures. Today already, Armis plays a role in:

- Protecting critical infrastructure by securing the entire range of digital products, including IoT and OT devices, which are often found in healthcare, industrial, and energy sectors. Armis is empowering enterprises to stay ahead of cyber threats, using experience gathered in 40+ critical infrastructure industries to fuel innovation that ensures their digital assets and operations remain secure in the constantly evolving digital landscape.
- Offering real-time insights and incident response to minimize damage from cyberattacks targeting critical systems.

By leveraging its strength in asset discovery, monitoring of connected devices and remediation of all security findings, Armis is instrumental in helping manufacturers and businesses meet the stringent cybersecurity requirements of the Cyber Resilience Act.

The Path Forward

Following its adoption, the legislative process will see the Act signed by the presidents of the Council and the European Parliament, with its publication in the EU's official journal due shortly. The regulation will take effect 20 days post-publication, with full application set for 36 months later, although some provisions may be implemented sooner.



Conclusion

The Cyber Resilience Act is more than just a legislative milestone; it's a critical step toward securing the digital future. As businesses and consumers prepare for its implementation, the focus will remain on safeguarding digital products and networks in an increasingly interconnected world. For stakeholders in the digital economy, understanding and adapting to these changes is not just necessary—it's imperative.

Engagement with the Act's provisions now will ensure readiness and resilience in the face of evolving cybersecurity challenges, paving the way for innovation and trust in the digital age.