Cytiva
100 Results Way
Marlborough MA 01752
USA

23 June 2026

Cytiva's Commitment to Cybersecurity Under the EU Cyber Resilience Act

As the cybersecurity landscape evolves, security expectations placed on product manufacturers increase. The European Union's Cyber Resilience Act (CRA) represents a significant step forward in establishing consistent cybersecurity requirements across the entire product lifecycle. At Cytiva, we recognize both the importance of this regulation and the responsibility it places on us to ensure our products are secure, resilient, and trustworthy.

Our approach is grounded in the principle that cybersecurity must be built into our products from the very beginning. This includes performing risk-based assessments, implementing secure architectures, and minimizing potential attack surfaces. Consistent with the expectations set forth in the CRA, our products are intended to be placed on the market without known exploitable vulnerabilities at the time of placing on the market and with appropriate safeguards to protect the confidentiality, integrity, and availability of data.

Before a product is placed on the market, Cytiva applies processes intended to align with applicable regulatory requirements, including those defined by the CRA. This includes completing the necessary conformity assessments, maintaining technical documentation in accordance with the CRA, and issuing an EU Declaration of Conformity and affixing CE marking where required.

Cytiva also recognizes that cybersecurity does not end when a product is delivered. The CRA places strong emphasis on lifecycle security, and our commitment extends throughout the operational life of our products. Cytiva provides ongoing security support, including the development and release of updates and patches without undue delay and free of charge during the support period, and actively monitors emerging threats and vulnerabilities that could impact our products. This ongoing effort is essential to helping ensure that our products continue to meet regulatory expectations and maintain an appropriate level of cybersecurity over time.

An important pillar of Cytiva's approach is how vulnerabilities are managed. Cytiva maintains structured processes for identifying, assessing, and addressing potential security issues, whether they are discovered internally or reported by external researchers or customers. Reports are evaluated using risk-based criteria, and remediation actions are prioritized accordingly. In line with industry practice and the expectations of the CRA, Cytiva supports coordinated vulnerability disclosure by maintaining a policy for coordinated vulnerability disclosure and by providing single point of contact for reporting potential issues. Cytiva also communicates appropriately with stakeholders as vulnerabilities are addressed. Additionally, Cytiva takes reporting of discovered vulnerabilities seriously, as such we are a CVE Numbering Authority (CNA). This allows us to publicly share vulnerabilities within our products.

Where required, Cytiva is taking steps to ensure we meet regulatory obligations for reporting cybersecurity incidents and actively exploited vulnerabilities to the appropriate authorities within defined timelines. These requirements reinforce transparency and support the broader ecosystem in responding to cybersecurity risks.

Transparency with our customers is another critical aspect of Cytiva's commitment. Cytiva provides product documentation and user information designed to support secure deployment and operation, including guidance on configuration, update management, and security considerations.

Ultimately, cybersecurity is a shared responsibility. While Cytiva is committed to delivering secure and resilient products, customers are encouraged to follow recommended security practices, including applying updates, configuring products securely, and promptly reporting any suspected vulnerabilities or incidents. Working together, we can maintain a strong security posture and reduce risk across the entire product lifecycle.

Cytiva is dedicated to supporting the CRA`s objectives through ongoing investment in secure development, lifecycle security, and responsible vulnerability management, and to engage constructively with customers, regulators, and broader security community to continuously raise the bar for product cybersecurity.

Robert Herrmann

Robert Herrmann
Director, Product Security

Disclaimer: This document provides a general overview of Cytiva's approach to cybersecurity and regulatory alignment. Specific product requirements, support periods, and security capabilities may vary by product and are defined in product-specific documentation. This document does not constitute a legally binding commitment and should be read in conjunction with applicable product documentation and contractual terms.