SOLUTION BRIEF_

ECLYPSIUM SOLVES CHALLENGING EU CYBER RESILIENCE ACT REQUIREMENTS

How Eclypsium Delivers CRA Compliance for Hardware and Firmware Inventory and Supply Chain Security

The EU Cyber Resilience Act, (Regulation 2024/2847) which entered into force in December 2024 and will be fully enforced by December 2027, fundamentally changes cybersecurity due diligence requirements and vulnerability handling responsibilities throughout the digital supply chain.

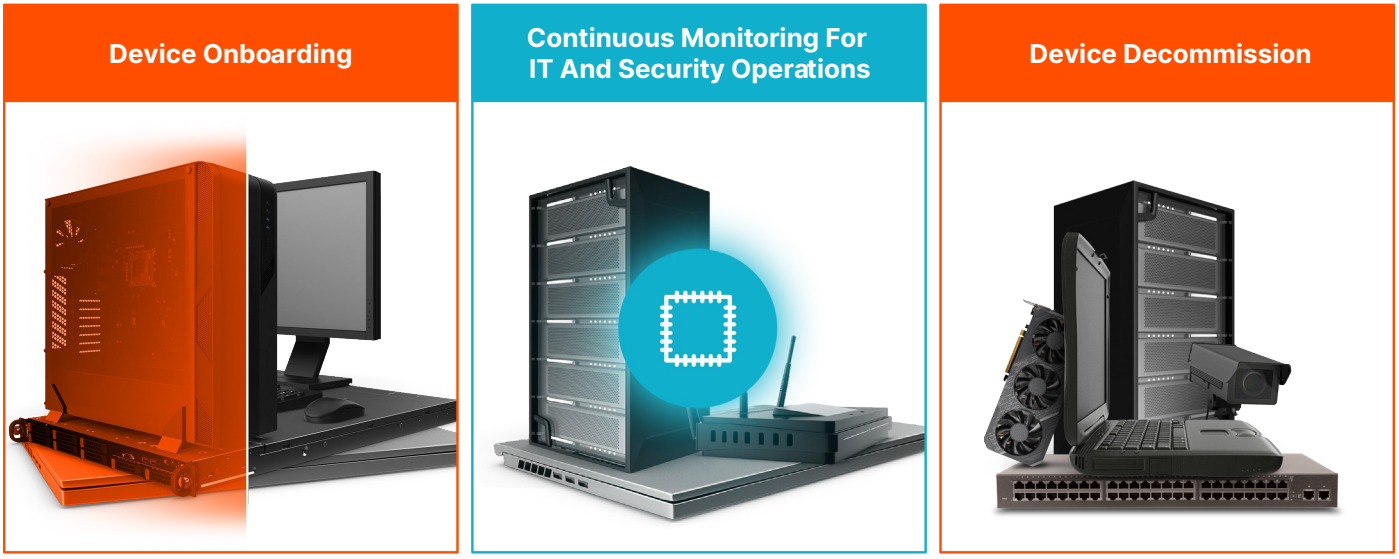
Organizations that bring "products with digital elements" to market are required to conduct rigorous due diligence against all digital elements in their products, and can become liable for vulnerabilities in "all integrated components" – including firmware and hardware components they didn't manufacture and may not be able to directly access or patch. This creates immediate compliance challenges for enterprises and technology vendors that current security and supply chain technologies may not be able to meet.

The current technology landscape for both generating and using Software Bills of Materials, as well as for vulnerability handling at the "integrated component" level, such as hardware and boot managers, is lacking. Eclypsium delivers necessary capabilities for achieving CRA compliance.

CRA Requirement	What Eclypsium Does
Security Due Diligence Manufacturers must assure that digital elements and integrated components, including those from third parties and free, open source software, meet the essential cybersecurity requirements of the CRA, including being free of vulnerabilities, receiving regular security updates, and other security tests.	**Scan Devices and All Integrated Components for Versions and Vulnerabilities** Eclypsium scans devices, and their component digital elements, to verify that they have the most up-to-date firmware, and that the firmware is free of other known and unknown vulnerabilities. Eclypsium checks whether the firmware version matches the latest published version from the manufacturer. Eclypsium monitors the integrity and security of devices throughout the entire lifecycle, from procurement and deployment through operational lifetime and disposition.
Comprehensive SBOMs with Firmware Coverage Organizations must document all digital elements in their environment, including firmware components that traditional tools cannot detect or inventory accurately.	**Complete SBOM Generation with Hardware and Firmware Visibility** Eclypsium automatically scans deployed environments to extract comprehensive SBOMs that include software, firmware, and hardware components actually present in your infrastructure. Instead of relying on manufacturers to provide accurate documentation, Eclypsium discovers what's actually running in enterprise environments, including firmware versions that may have been modified or contain undocumented or counterfeit components. Most SBOM generation tools lack visibility into hardware, firmware, and components within digital products. Eclypsium sees it all.

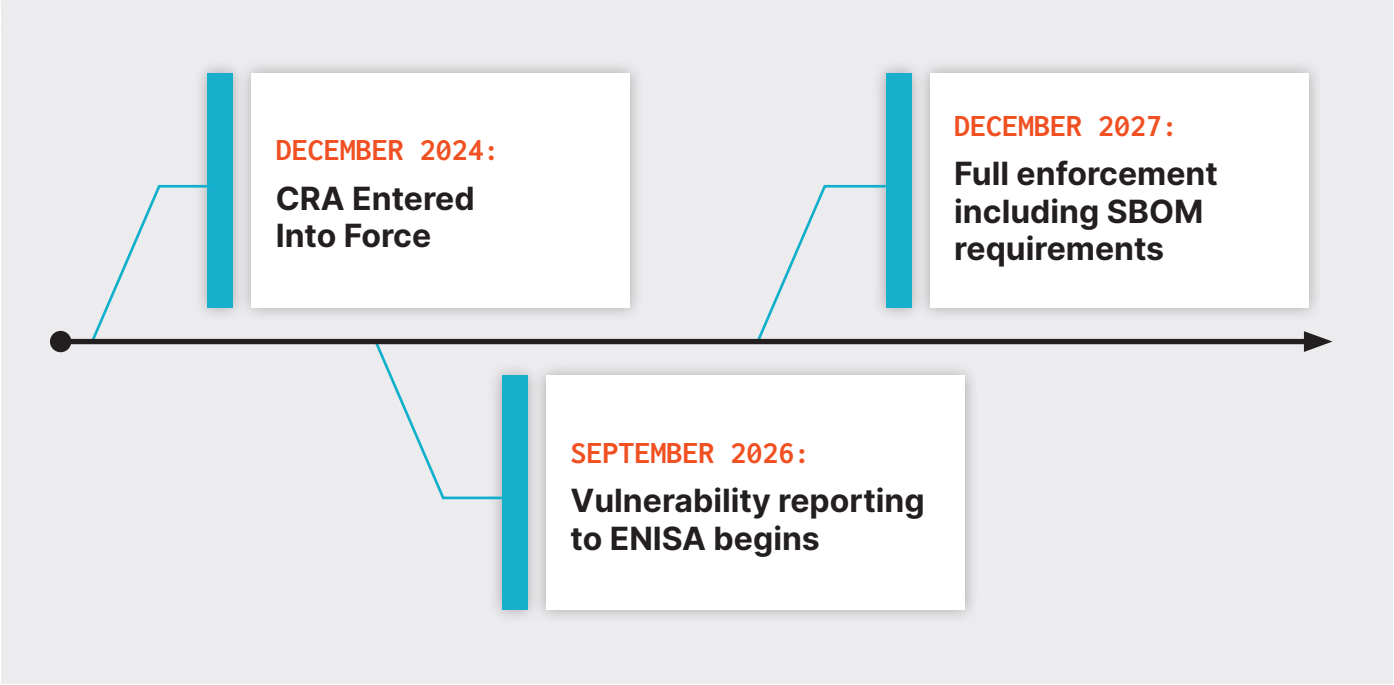
CRA Requirement	What Eclypsium Does
Vulnerability Management Across "All Integrated Components" The CRA requires timely identification and remediation of vulnerabilities in every component of a digital product, regardless of whether the organization manufactured that component or has direct access to its source code.	**Component-Level Vulnerability Detection Beyond Version Matching** Traditional vulnerability management fails when firmware versioning is inconsistent across the supply chain. Eclypsium extracts and decompiles firmware binaries from endpoints, network devices, servers, and AI hardware to identify both known and previously unknown vulnerabilities. This approach works regardless of version numbering inconsistencies and catches vulnerabilities that version-matching approaches miss entirely.
Supply Chain Accountability and Rapid Response When vulnerabilities are discovered, organizations must notify upstream suppliers and provide fixes where possible – but the law acknowledges that many supply chains contain multiple layers where this becomes practically impossible.	**Supply Chain Risk Assessment and Vendor Accountability** By providing deep analysis of the actual firmware deployed in your environment, Eclypsium enables organizations to hold upstream supply chain vendors accountable for vulnerabilities in their products. Rather than accepting vendor assurances about security, organizations can verify the actual security posture of deployed components and demand specific fixes for identified vulnerabilities.
Securing Digital Elements with Cybersecurity Impact The CRA specifically notes the added risk of digital elements like boot managers which serve cybersecurity functions. If a boot manager is compromised, it undermines nearly all other cybersecurity controls in place.	**Eclypsium Monitors for Bootkits and Boot Process Malware** Cyberattackers love to compromise the boot process of digital devices because it gives them great control while keeping them hidden from detection by cybersecurity tools. Eclypsium monitors UEFI, Secure Boot, and other "Below the OS" processes to prevent adversaries from hiding their malicious actions and persisting after OS reinstalls and other remediation steps.

Eclypsium Delivers Protection at Every Link in the Digital Supply Chain_



Continuous Trust For Enterprise Hardware Throughout Lifecycle

CRA Timeline and Immediate Action Required_



Organizations need to begin building CRA compliance capabilities now. The complexity of achieving comprehensive firmware visibility and vulnerability management across complex supply chains requires time to implement and operationalize.

Ready to see how Eclypsium addresses your specific CRA compliance requirements?

Request a demo to understand how our platform works with your current infrastructure and supply chain relationships.

About Eclypsium_

Eclypsium's cloud-based platform provides digital supply chain security for critical software, firmware and hardware in enterprise infrastructure. Eclypsium helps enterprises and government agencies mitigate risks to their infrastructure from complex technology supply chains. For more information, visit eclypsium.com.