BLACK DUCK®

NAVIGATING THE EU CYBER RESILIENCE ACT WITH BLACK DUCK

A COMPREHENSIVE APPROACH TO PRODUCT SECURITY

WHAT IS A PDE?

Products with digital elements include any software or hardware product that has direct or indirect data connectivity and includes digital components that are essential for its function.

- Smartphones, laptops, and IoT devices
- Industrial control systems
- Smart TVs, connected cameras, smart thermostats
- Mobile apps, desktop applications, and embedded firmware

The European Union's Cyber Resilience Act (EU CRA) introduces significant new requirements for software producers, aiming to ensure transparency, vulnerability management, and long-term security maintenance guidelines for products with digital elements (PDEs). These new requirements put additional pressure on organizations to prioritize product quality and security throughout the entire product life cycle, from development to post-market monitoring. Meeting these demands can be challenging, particularly for companies without mature application security (AppSec) programs, and can lead to compliance costs, financial penalties, market delays, and increased risk.

KEY EU CRA REQUIREMENTS

Security by design and default

PDEs must be designed, developed, and produced with an appropriate level of cybersecurity based on risk assessment. Products must be placed on the market without known exploitable vulnerabilities and with a secure-by-default configuration.

Vulnerability handling and reporting

The CRA mandates robust vulnerability management processes throughout the product's life cycle. This includes continuous monitoring, regular testing, addressing vulnerabilities without delay, and establishing a coordinated vulnerability disclosure policy. Additionally, manufacturers must notify the appropriate EU agency of any actively exploited vulnerability within 24 hours of becoming aware.

SBOM provision

Manufacturers must identify and document the components contained in their products, which includes producing Software Bills of Materials (SBOMs). These SBOMs must be in a commonly used, machine-readable format and cover, at minimum, direct application dependencies.

Conformity assessment

Before a PDE can be sold in the EU, manufacturers must conduct a conformity assessment to demonstrate compliance with the CRA's essential requirements.

BLACK DUCK'S CRA SOLUTION

Black Duck's AppSec portfolio provides a unified, automated security approach that analyzes both proprietary source code and external dependencies, identifying vulnerabilities and quality issues early and continuously throughout the software development life cycle. This combined insight, coupled with seamless development integrations, enables effective prioritization and remediation, aligning with regulatory timelines and expectations.

CRA Requirements	Black Duck Solutions
Security by design and default	• Static application security testing (SAST) detects design and code-level flaws early • Fuzz testing uncovers runtime security issues • Software composition analysis (SCA) identifies vulnerable external dependencies
Vulnerability handling and reporting	• SCA alerts on known vulnerabilities and malicious packages • Fuzz testing surfaces zero-day vulnerabilities
SBOM provision	• SCA automatically identifies dependencies and exports SBOMs in standardized formats
Conformity assessment	• SCA, SAST, and fuzz testing offer detailed reports of tests, findings, and component usage • Application security posture management (ASPM) provides a consolidated view of all testing performed on an application

Solution highlights

- **Black Duck® SCA** scans applications to identify open source and third-party dependencies, and alert teams to associated security, license compliance, or component health risks. Black Duck SCA also generates SBOMs in SPDX or CycloneDX formats, with standard or custom fields. And it provides detailed documentation of applications scanned, risk findings, and component usage.
- **Coverity® Static Analysis** analyzes proprietary source code to detect and remediate quality and security coding flaws early, supporting secure-by-design development. Coverity can also produce compliance reporting for standards including ISO 26262, CERT C/C++, and MISRA.
- **Defensics® Fuzzing** uncovers unknown vulnerabilities in protocols and interfaces through generative fuzz testing techniques including rigorous fault injection, helping validate product robustness, stability under adverse conditions, and resilience.
- **Software Risk Manager™** is an ASPM tool that provides a consolidated record of all application security testing performed on a product. This security system of record includes test result support from over 150 tools and is a key provider of information to quality management systems.

Why Black Duck

Black Duck is a seven-time Leader in the Gartner® Magic Quadrant™ for Application Security Testing, a five-time Leader in the Forrester Wave™ for Software Composition Analysis, and a three-time Leader in the Forrester Wave™ for Static Application Security Testing. Black Duck has a proven track record of helping software and hardware manufacturers comply with regulatory and safety standards, such as those in automotive, industrial, medical devices, and aerospace and defense industries. Black Duck's comprehensive portfolio, high-fidelity results, and dedicated support team make it the top choice for software producers needing confidence in their adherence to CRA requirements.

Read more about how Arm trusts Black Duck to navigate CRA requirements

ABOUT BLACK DUCK

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.