Future-Proofing Cybersecurity:

Payara's Response to the EU Cyber Resilience Act

The Cyber Resilience Act (CRA) will become law in Europe in 2024 and Payara is actively working to assist our customers to be well informed and ready to work toward compliance with this new legislation. Affected manufacturers will be required to apply the legislation 36 months after its publication by the Office of the European Union.

EU and non-EU vendors selling a product or service with a digital component, including software – and who export to the EU – are required to comply.

What is the Purpose of the EU Cyber Resilience Act?

A key objective of the CRA is to ensure a common and high level of cybersecurity for connected products ("products connected directly or indirectly to another device or network" as per the EU Cyber Resilience Act definition) made available on the European market. This will be achieved through the development and implementation of harmonized cybersecurity standards applicable to such products – throughout their lifecycle.

The Cyber Resilience Act's aim is to:

"impose cybersecurity obligations on all products with digital elements whose intended and foreseeable use incudes direct or indirect data connection to a device or network" (EU cyber-resilience act, Briefing – 28-11/2023)

Are There Penalties for Non-Compliance?

Non-compliant companies can be fined $15 million or 2.5% of their global annual turnover – whichever is higher. Authorities may also intervene with orders to eliminate risk, restrict the product, or even issue a product recall.

The Risks of Using the Payara Platform Community for Secure and Compliant Applications

While the Payara Platform Community Edition is geared towards rapid development and innovation, its frequent changes and evolving features pose significant challenges for those seeking long-term stability and regulatory compliance. Unlike Payara Platform Enterprise and Payara Cloud, the Payara Community Edition lacks the comprehensive compliance features required to meet stringent regulatory standards, including CRA, making it an unsuitable choice for applications where security and compliance are imperative.

What Payara Products Should I Use to Ensure Compliance?

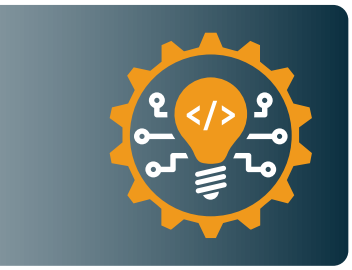
Users should consider the Payara Platform Enterprise or Payara Cloud. Those products are specifically designed for mission-critical systems where stability, security, and compliance are paramount. Payara Platform Enterprise offers long-term support with a stable release cycle, ensuring that APIs and features remain consistent and reliable over time. Additionally, it includes extensive compliance and security features to meet stringent regulatory requirements. With professional support, regular maintenance updates, and guaranteed response times, Payara Platform Enterprise provides the robustness and assurance needed for enterprise-level applications. This makes it the optimal choice for organizations that prioritize operational continuity and regulatory adherence.

How Does Payara Support Its Customers to Achieve Compliance?

Payara's application server technology plays an important role in the operation of many software applications or related products that may fall within the scope of the CRA. We have been closely following the evolution of the legal requirements and we understand that our customers may need our assistance to help them work towards fulfilling their own compliance objectives. For example, products within the scope of the CRA must undergo a written "conformity assessment"; affix a conformity mark to their product; conduct cybersecurity risk assessments; provide security updates free of charge for five years; report vulnerabilities; and disclose any successfully exploited vulnerabilities within 24 hours.

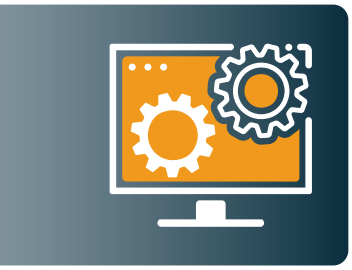
At Payara, we constantly enhance our cybersecurity measures to meet top standards. Our products—Payara Server, Payara Micro Enterprise Edition, and Payara Cloud—come with essential features and configurations to strengthen your security. **Key highlights include:**

With appropriate configuration when running on compliant hardware and software infrastructure (including the operating system and the Java virtual machine, both of which are outside the control of Payara), Payara supports the NIST Federal Information Processing Standards (FIPS). This will be of particular interest since it's often a prerequisite for those supplying software solutions to the U.S. government.



The Payara Platform, as a compliant implementation of Jakarta EE, supports Jakarta Authentication and Authorization, as well as the Jakarta Security API. Developers can build using the OIDC (OpenID Connect) protocol and then support single-sign-on schemes such as Google, Facebook and others in their Payara deployed Jakarta EE applications.

Our monthly product releases help you ensure that the software components in your supply chain are up-to-date and therefore as free of Common Vulnerabilities and Exposures (CVEs) as possible. (The current list of CVEs is maintained by the MITRE Corporation and is funded by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)).



As a Java software and Jakarta EE implementation, the Payara Platform complies with security specifications such as JAAS (Java Authentication and Authorization Service) and JACC (Java Authorization Contract for Containers).

We prioritize security and follow best practices in line with ISO 27001 standards, such as adherence to OWASP (Open Web Application Security Project) guidelines.

Further Information

Guidance from the executive branch of the EU, the European Commission, regarding how the CRA will be applied will be available once the law is in force.

We look forward to keeping you informed about important cybersecurity legislation, regulations and industry standards in the months and years ahead. If you have any questions, don't hesitate to contact us at info@payara.fish

Sign up for updates or contacts us if you have any questions on https://www.payara.fish/cyber-resilience-act/

Issued in **June 2024**