The European Union Cyber Resilience Act- A concrete step towards reinforcing the foundational security in the ever-expanding digital landscape

Regulation (EU) 2024/2847 of the European Parliament and of the Council

Modern digitalized businesses and supply chains present increasing IT vulnerabilities and risks amid rapid adoption of technology products. From smart products to IAM systems, and from foundational IT infrastructure to high-value systems in place, the European Union (EU) Cyber Resilience Act (CRA) provides comprehensive guidelines to protect and secure products with digital elements (PDE). **The regulation lays out the legal framework for essential cybersecurity requirements for placing products with digital elements on the market.**

This objective of this legislation is to enhance cyber resilience in an era when businesses across wide-ranging sectors are witnessing proliferation of IT systems-software and hardware, to run day-to-day operations, which in turn results in technology and cyber vulnerabilities.

Table of content

The European Union Cyber Resilience Act: Lets delve deeper into the Act

Synopsis

The European Union is amid a fast-changing cybersecurity regulatory landscape. As business and government organisations turn increasingly digital, the threats presented by exponential growth of inter-connected devices are increasing. Considering the humungous challengers posed by this transformation, the Union has mandated a comprehensive list of guidelines to overcome cyber threats and vulnerabilities to protect the Union's economy, its businesses and people in general which includes consumer privacy along with health safety from underlying cyber threats. Broadly, these comprehensive set of guidelines, which is known as, The EU's Cyber Resilience Act (Regulation EU 2024/2847) 'CRA' are intended to ensure that

- The Union's consumer rights are protected by ensuring the PDEs that are placed on the market are safe and secure by design, development and configuration including the entire product lifecycle (maintenance, upgrade and support)
- That there are boundary conditions for the development of secure products with digital elements both hardware and software by ensuring that these PDEs are with fewer vulnerabilities
- The manufactures take security issues seriously
- Furthermore, and more importantly, it strives to create conditions to take cybersecurity measures into account when selecting and using products with digital elements

The scope of the EU Cyber Resilience Act and why it is such a significant step forward?

The Act is very broad in its scope, covering the entire supply chain in the Union, encompassing the manufacturing units, importers and distributors of products with digital elements (PDEs).

Furthermore, the act is more practical in terms of implementing. The reason being that while existing Union law applies to certain products with digital elements, there is no horizontal regulation applicable across the Union that establishes comprehensive cybersecurity requirements for all products with digital elements.

What are the essential requirements to comply with the EU CRA

The essence of the CRA is that the software or hardware that is made available on the market should be without any exploitable vulnerabilities. As per the regulations, the software or hardware vendor is obliged to make a risk assessment before the solution is made available in the market.

Annexure 1 of the Act lays out requirements necessary to abide by security requirements. The list of requirements is all encompassing and broadly include the following requirements.

PDEs must be without known exploitable vulnerabilities and with secure configuration unless otherwise agreed between the manufacturer and the user to tailor made a product.

- PDEs must ensure that vulnerabilities can be addressed through security updates,
- PDEs must ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorized access
- PDEs must protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means
- PDEs protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, and report on corruptions
- (g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimization)
- (h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks
- (i) minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks
- (j) be designed, developed and produced to limit attack surfaces, including external interfaces
- (k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques
- (l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user
- (m) provide the possibility for users to remove on a permanent basis all data and settings securely and easily and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner

Which products are categorized as products with digital elements?

The CRA recognizes that PDEs bear certain amounts of risk based on the nature of software and hardware. Accordingly, it lists PDEs under high risk and critical risk categories. The high-risk category includes PDEs such as:

1)Identity and Access Management systems
2)Privileged Access Management systems
3)Password Managers
4)Virtual Private Network
5)Operating Systems
6)Microprocessors and microcontrollers

The critical-risk category includes PDEs such as:

- Hardware devices with security boxes
- Smartcard or similar devices
- Smart Meter Gateways

Why identity-first security will be at the core of the new policy guidelines

Today identity is at the core of digital transformation. Human and machine identity continuously interact with data, AI models, machines, scripts, codes, APIs, IT infrastructure, cloud resources such as admin consoles, containers among others. Identities also play crucial roles in cyber physical landscape as well as industrial internet of things. Any anomalous identity-based attack or absence of robust authentication mechanisms can lead to loss of reputation, confidential information and business agility.

To counter these challenges, in today's highly complex digital environments, the foundation of a robust cybersecurity framework can be built by implementing an Identity-first security approach. To manage identity-centric controls in on-prem or on-cloud environments, organizations can count on an Identity-first security approach, that ensures context-wise controls and continuous monitoring of the identities, for both supply chain management, digitalization, or cloud migration. ARCON believes that Privileged Access Management (PAM) is an absolute must to build the identity-first security architecture.

The solution plays a pivotal role in managing risks stemming from compromise of privileged identity. Indeed, a privileged identity often includes permissions that allow changes to be made to settings, such as security configurations.

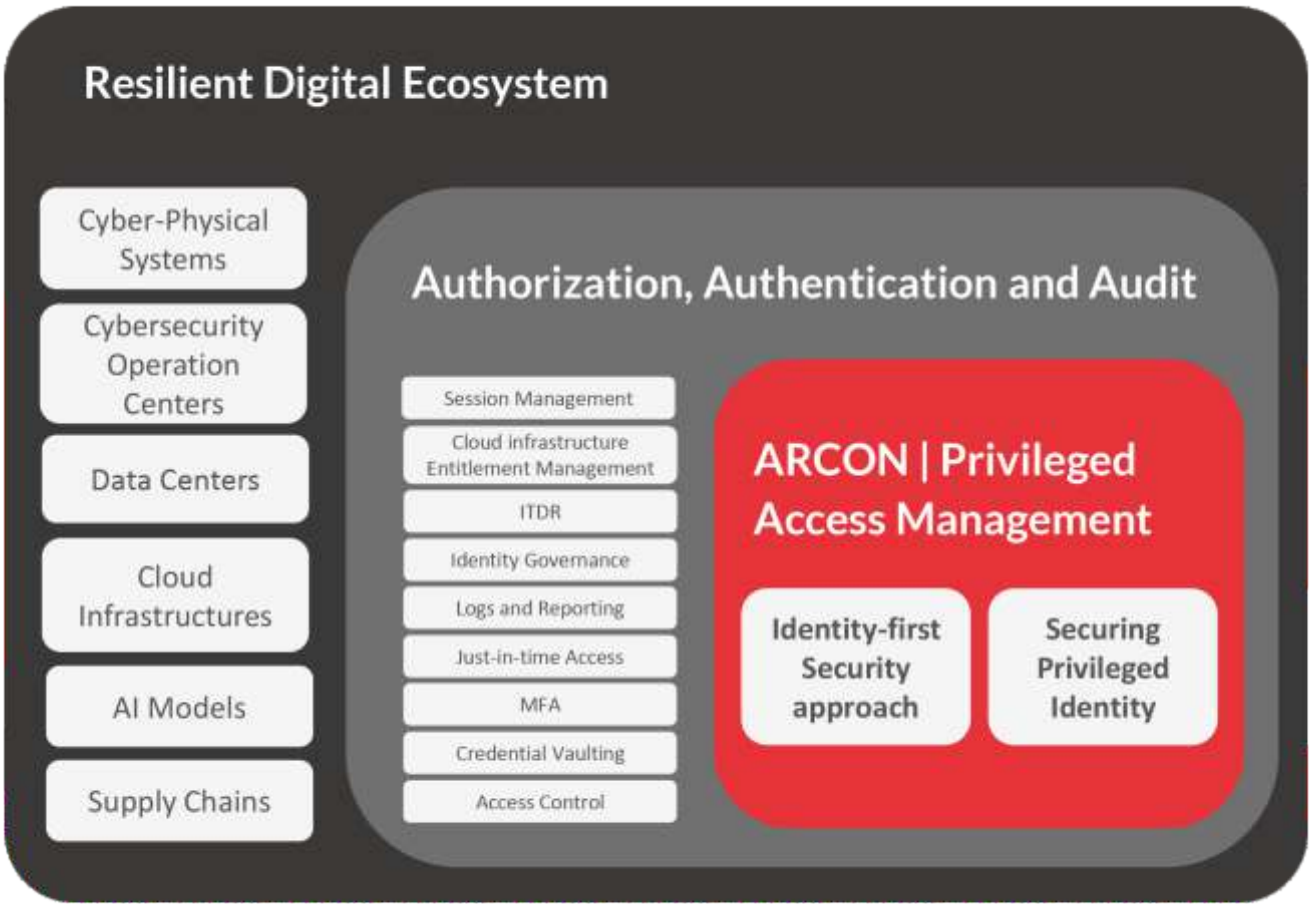
How ARCON Privileged Access Management complies with the EU's CRA

"All products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered to be less critical can facilitate the initial compromise of a device or network, enabling malicious actors to gain privileged access to a system or to move laterally across systems. Manufacturers should therefore ensure that all products with digital elements are designed and developed in accordance with the essential cybersecurity requirements laid down in this Regulation." **EU Cyber Resilience Act**

It is quite evident that secure privileged access to systems will play a big role in complying with the EU CRA. Indeed, if one must consider that identity is at the core of every human and machine interaction with inter-connected devices, applications, and what a central component a Privileged Access Management systems has become lately against the backdrop of increasing demand for data security and privacy, we believe that, a comprehensive PAM solution with a very secure architecture, will go a long way in building a robust security posture for building cyber resilience.

ARCON | Privileged Access Management has born out of datacenter. ARCON understands the complexities involved in managing privileged access across widely distributed systems and the importance of secure access to business and infrastructure applications. Therefore, ARCON has designed and developed its PAM solution with the broadest range of features and functionality to address organizations' cyber resilience initiatives. ARCON Privileged Access Management Solution is designed to address the challenges of privileged identities and provides an added layer of security to help build in controls that ensure access only on a "need-to-know" and "need-to-do" basis. The PAM solution has several components; and the major components are Access Control, Multifactor Authentication, Credentials Management, Just-in-Time privileges, Audit Trails, Session Management and Identity Threat Detection and Response (ITDR). It enables IT security professionals to build a solid perimeter security around IT systems, endpoints, and data whilst enabling them to develop a comprehensive Governance, Risks, and Compliance (GRC) framework.

By nature, privileged accounts have the greatest potential for operational risk, business continuity risk, reputational risk, loss of intellectual property, loss of regulated data or even, in the case of cyber-physical and IIoT incidents resulting in catastrophic loss.



Furthermore, ARCON | PAM is designed, developed and supported by robust security protocols that ensure cyber vulnerabilities are kept at bay.

Timely Upgrades:

We have a highly effective OCI that handles upgrades for all components, including the application and database, with a very high success rate. The OCI is designed to manage both upgrades and rollbacks, providing a seamless transition in case of any issues. A rollback mechanism is a safety net that allows you to revert to a previous version in case of unexpected problems post-deployment. This feature ensures minimal disruption to operations.

CI/CD Pipelines:

A Continuous Integration and Continuous Deployment (CI/CD) pipeline is critical for delivering updates swiftly and reliably. Implementing automated build, test, and deployment processes streamlines the journey from code changes to production release. For a Software-as-a-Service (SaaS) offering and cloud deployments, this pipeline ensures a consistent and efficient release cycle.

Software Quality:

Adopting a multi-layered testing approach minimizes the risk of defects reaching the production environment. Our testing strategy encompasses multiple rounds of Quality Assurance (QA) and functional testing. This ranges from unit and integration tests at the microservice level to

comprehensive QA checks and user acceptance testing before rolling out any patches or updates. ARCON | PAM has adopted the Security Common Criteria EAL Level 2+ standard and registered for testing by STQC Labs, India the certification testing for which is currently under progress at Bangalore. ARCON | PAM has got 27001 (ISMS) and 9001 (QMAS) certifications ensuring that our organizational processes are planned in such a manner that ensures security from the base level in the development of the product. ARCON | PAM SaaS operations have also received SOC 2 Certification for all regions. Note: FIPS- 197, FIPS- 140, NIST 800-57: ARCON has been validated for these standards by independent auditors and complies with these standards.

Support:
ARCON provides 24/7 support to all its customers across the globe. We have a single gold level standard support as the company believes that this is a critical element in the PAM space. ARCON provides training in line with clients' requirements on both online and offline methodology on a regular basis.

Training:
ARCON University which is the online Learning Management Systems offers Certification for PAM Basics, PAM Administrator, PAM Implementor and PAM Professional. ARCON publishes many FAQs and training videos on its support portal. ARCON has also started to push Training Videos as part of the solution offering for Enterprise Customers.

The Timeline

The EU CRA came into force on December 10, 2024. The act, however, will be applicable in a phased manner.

- June 11, 2026: Provisions relating to conformity assessment bodies will start to apply.
- September 11, 2026: Manufacturer's obligation to report vulnerabilities will commence.
- December 11, 2027: The Act will be fully implemented.

Penalties for Non-compliance

- Non-compliance with the essential cybersecurity requirements can result in a fine up to EUR 15 million or up to 2.5% of the offender's worldwide turnover.
- Non-compliance with other obligations can result in a fine up to EUR 10 million or up to 2% of the offender's worldwide turnover.
- Providing misleading or incorrect information to market surveillance authorities or a relevant body can result in a fine up to EUR 5 million or 1% of the offender's worldwide turnover.

The EU CRA will complement NIS 2 Implementation

The EU CRA will very well complement the EU's Network and Information System 2 Directive (NIS 2). As NIS 2 Guidelines require operators of critical infrastructure and essential services to implement appropriate security measures and report incidents in timely manner, implementation of EU CRA, that is, deployment of products with digital elements without any security vulnerabilities will go a long way in building the security posture and help adhere to the NIS 2 directive.

Conclusion

Amid an increasingly stringent regulatory landscape, operators of critical services and infrastructure including financial organizations are obliged to build a robust cybersecurity program and adopt appropriate measures to mitigate vulnerabilities. To address these challenges, it is imperative to have robust privileged access management in place. ARCON | Privileged Access Management (PAM), a critical product with digital element in addition to adhering to the EU CRA, directly helps in implementing the NIS 2 Guidelines.

About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.