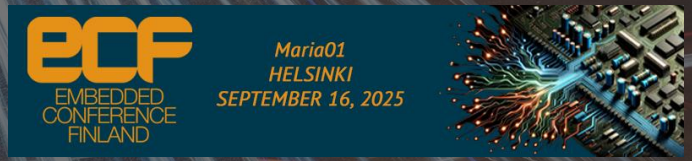
CYBERSECURITY REGULATIONS: A PARADIGM SHIFT

Meeting the EU Cyber Resilience Act with insights from Digi International — ensuring a clear path to compliance!



Agenda

1. Introduction to the EU Cyber Resilience Act (CRA)
2. Main CRA pillars
3. Timeline / Main Milestones
4. Key CRA requirements and reporting obligations
5. Complying with CRA, leveraging Digi security building blocks
6. Wrap-up and questions

Introduction to the EU Cyber Resilience Act (CRA)

EU Cyber Resilience Act (CRA) - Regulation (EU) 2024/2847

- **The CRA fundamentally alters the landscape of product compliance in the EU**
  - Integrating robust cybersecurity measures into the existing framework for CE marking
  - Mandatory for any product or software that contains digital elements
  - Manufacturers and retailers, both have responsibility
  - Throughout the entire product lifecycle
- **Twofold problem addressed**
  - Poor levels of cybersecurity in products or inadequate security updates
  - Inability of consumers and businesses to determine which products are secure or how to set them up to ensure they are protected
- **What will CRA guarantee?**
  - Harmonized rules when launching products or software with a digital component
  - Cybersecurity requirements framework governing the planning, design, development and maintenance of such products
  - Obligation to provide a duty of care throughout the entire product lifecycle
- **What happens if products do not comply?**
  - No qualification for CE marking, no authorization for sale in the EU
  - Possible recall or withdrawal of products
  - Penalty payments (up to 2.5% of total annual turnover worldwide)

Main CRA Pillars Overview

Stricter Cybersecurity

Design, development, maintenance and EOL; proactive removal of vulnerabilities and recurring updates

Conformity Assessments

Detailed assessments to ensure compliance with cybersecurity requirements

Transparency and Communication

Clear and up-to-date information on product security features and any relevant security issues

Early Vulnerability Notifications

Any actively exploited vulnerability discovered must be reported to authorities within 24 hours of its detection

Supervision and Audits

More intensive to ensure continued compliance with cybersecurity requirements

Product Classification

Different categories according to their level of risk (default, important and critical)

Countdown to CRA Compliance

December 14, 2020

Regulation announced in 2020 EU Cybersecurity Strategy (complements NIS2 Framework)

October 23, 2024

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

November 20, 2024

Publication of Regulation (EU) 2024/2847 in the official journal of the European Union

Countdown to CRA Compliance

December 10, 2024

CRA is officially adopted into EU legislation with a grace period before full adoption is mandatory.

June 11, 2026

- Conformity assessment bodies responsible for verifying CRA compliance become operational.
- Organizations should begin familiarizing themselves with conformity assessment procedures ahead of 2027 deadline.

September 11, 2026

- Article 14 (Reporting Obligations of Manufacturers) shall apply from this date.
- Report actively exploited vulnerabilities and severe incidents to national authorities (CSIRT) and ENISA within 24 hours.

December 11, 2027

- The Cyber Resilience Act officially comes into effect.
- All applicable products require a CE marking to be authorized for sale in the EU.

CRA Essential Cybersecurity Requirements

Ensure that products are designed, developed, produced and maintained in compliance with essential cybersecurity requirements (as per EU CRA – Annex I, Part I)

Secure by Design and Default

- Be free of known exploitable vulnerabilities at release
- Secure boot, access control mechanisms, secure default settings

Secure and Reliable Software Updates

- Signed updates, secure OTA delivery with integrity checks
- Rollback protection against downgrade attacks

Data Protection and Encryption

- Encrypt sensitive data in transit and at rest
- Apply data minimization, secure storage

Authentication and Access Control

- Secure credential management (e.g. password policies)
- Secure access to console and interfaces

Reporting Obligation — Early Vulnerability Notifications

Any actively exploited vulnerability discovered must be reported within 24 hours. Manufacturers must establish a vulnerability management and reporting process.

Vulnerability Monitoring and Detection

- Generate a software bill of material (SBOM)
- Regularly scan for new vulnerabilities
- Implement a vulnerability disclosure program

Vulnerability Analysis and Transparency

- Develop internal triage process to assess vulnerabilities, impact, and possible exploitation
- Share and publicly disclose information about fixed vulnerabilities

Compliance and External Reporting

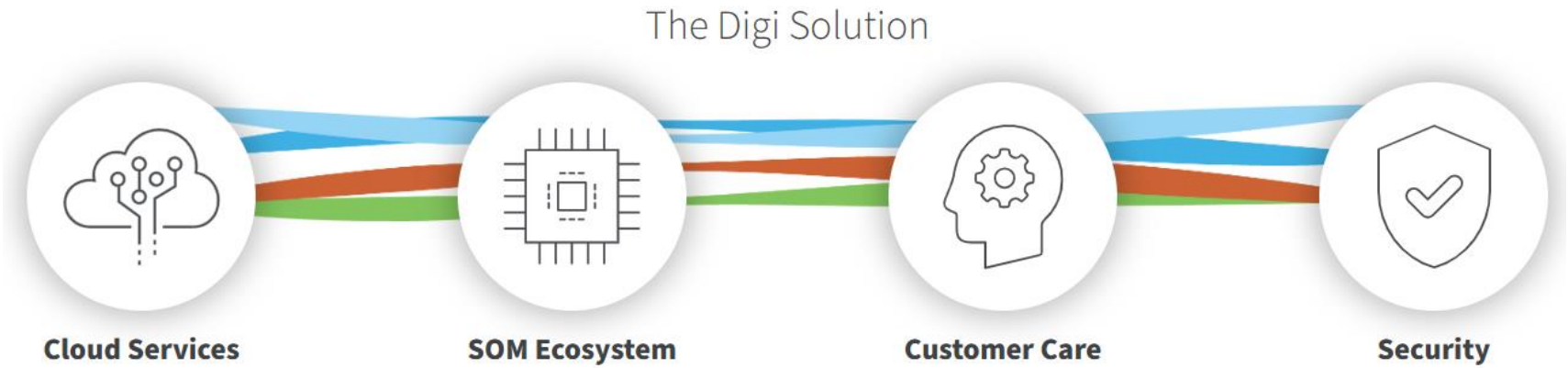
- Follow the CRA's mandated reporting timeline (report to ENISA and CSIRT)

Patch Management and Remediation

- Develop a patching strategy to address vulnerabilities within timelines
- Ensure remote update mechanisms for security updates

Digi ConnectCore — Secure Embedded Solutions

Digi's suite of embedded solutions are designed to simplify and accelerate the development, deployment and management of secure, connected devices that can be managed and updated throughout their lifecycle.



Digi ConnectCore — Security Building Blocks

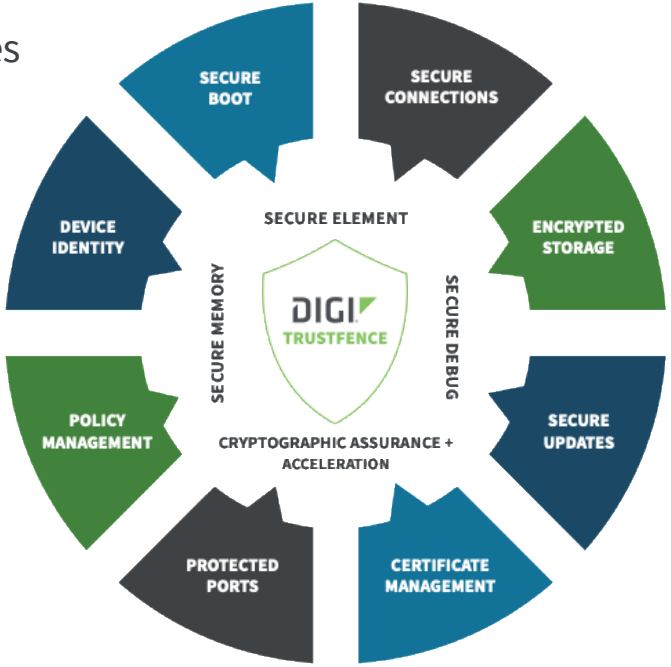
TrustFence®
Security Framework
to meet
“secure by design”
requirements

Digi ConnectCore®
Security Services
to address
vulnerability
management
requirements

Digi ConnectCore®
Cloud Services
to monitor and
update devices
without delay

Digi TrustFence® Security Framework

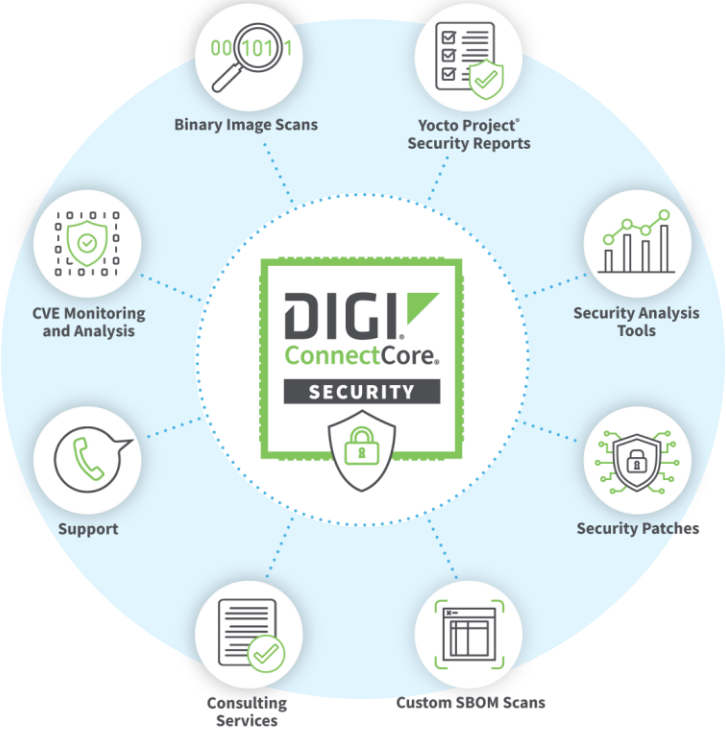
- Device security framework that simplifies securing connected devices
- Building on and leveraging SOC hardware security features
- Software integration in u-boot, kernel and user space
- Validated, optimized and easy to use
- Secure-by-design features
  - Secure Boot
  - Protected Ports
  - Tamper Detection
  - Secure / Encrypted Storage
  - Secure Firmware Update
  - Secure Element
  - Random Number Generators (RNGs)
  - FIPS Certification (selected platforms)



DIGI TRUSTFENCE®
START WITH BUILT-IN SECURITY.

Digi ConnectCore Security Services

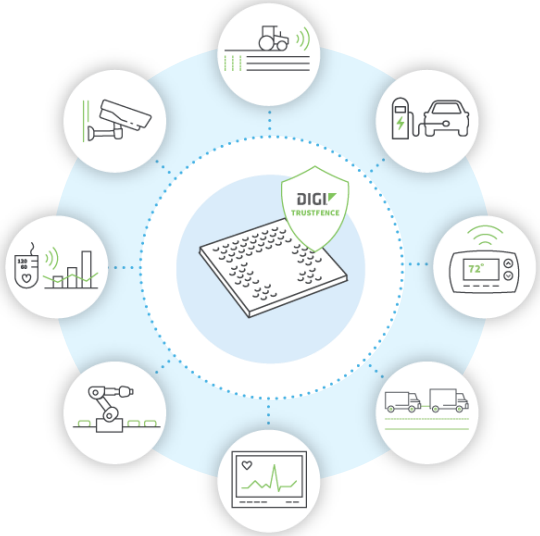
Maintain software security during entire product lifecycle



- Making security easier and more accessible
- Monitor and maintain security during **entire product lifecycle**
- Curated security analysis and visibility on DEY security status
- Identify security risks and vulnerabilities in **customer products**
- Support **SBOM management** (medical device requirements)
- **Binary image scans** for additional layer of security
- Security **software layer** including patches for common vulnerabilities
- **Engineering services** / consulting to remediate issues

Digi ConnectCore Cloud Services

Connect your device and create your own IoT Application



Wireless or wired Internet

TLS / Certificate-based authentication and encryption with 2048-bit RSA keys

DIGI ConnectCore CLOUD

Optional

Azure aws

Flexible APIs

TLS encryption with 2048-bit RSA keys

Service / management applications
End user applications
Custom dashboards

DEVICE | CLOUD | REMOTE APPLICATION

Digi ConnectCore Cloud Services

Connect your device and monitor and maintain it in the field

Key Features

- Remote OTA Firmware Updates
- Update Devices in Bulk
- Device Requests
- Templates / Zero-touch commissioning
- Automated Operations
- API Access
- File System Access
- System Monitoring
- Custom Data Streams
- Alarms and Alerts
- View and Group Devices
- Subaccounts
- Remote CLI
- Fixed price / device (no variable cost)

Complying with CRA leveraging Digi Security Building Blocks (I)

PART I	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(1)	Products shall be designed, developed and produced ensuring an appropriate level of cybersecurity based on the risks	✓ TrustFence overall	✓ Security Services overall	✓ Cloud Services overall	✓ DEY overall
(2) (a)	Products shall be made available without known exploitable vulnerabilities	N/A	✓ Custom SBOM scans, meta-digi-security	✓ Digi RM Vulnerability Patch Policy	✓ Digi owned software maintenance
(2) (b)	Products shall be made available with a secure by default configuration	✓ TrustFence overall	N/A	N/A	✓ *Hardened DEY reference image**
(2) (c)	Products shall ensure that vulnerabilities can be addressed through security updates	✓ Secure software update	✓ meta-digi-security, consulting & support	✓ Secure remote OTA software updates	✓ Secure software update, dual boot configuration
(2) (d)	Products shall ensure protection from unauthorized access	✓ Secure console, secure JTAG	N/A	N/A	✓ SSH/TLS
(2) (e)	Products shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other	✓ Encrypted file system / files (hardware bound)	N/A	✓ File system access, TLS, certificate-based authentication and encryption	✓ Encryption, WPA3, FIPS 140-2/3**

*Roadmap (coming soon)

**Additional cost involved

Complying with CRA leveraging Digi Security Building Blocks (II)

PART I	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(2) (f)	Products shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration	✓ Secure boot / authenticated file system	N/A	✓ File system access, TLS, certificate-based authentication & encryption	✓ TLS, read-only file system
(2) (g)	Products shall process only data, personal or other, that are adequate, relevant and limited to what is necessary	N/A	N/A	✓ Custom data streams	N/A
(2) (h)	Products shall protect the availability of essential and basic functions against denial-of-service attacks	N/A	N/A	N/A	✓ *Embedded systems security best practices**
(2) (i)	Products shall minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks	N/A	N/A	N/A	✓ *Embedded systems security best practices**
(2) (j)	Products shall be designed, developed and produced to limit attack surfaces, including external interfaces	✓ Secure boot, secure console, secure JTAG, tamper detection	✓ meta-digi-security, consulting & support	N/A	N/A

*Roadmap (coming soon)

Complying with CRA leveraging Digi Security Building Blocks (III)

PART I	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(2) (k)	Products shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	✓ Tamper detection	N/A	✓ Templates	N/A
(2) (l)	Products shall provide security related information by recording and monitoring relevant internal activity	✓ Tamper detection	N/A	✓ *Security monitoring agent**	N/A
(2) (m)	Products shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner	N/A	N/A	✓ File system access, DRM data/settings management	N/A

*Roadmap (coming soon)

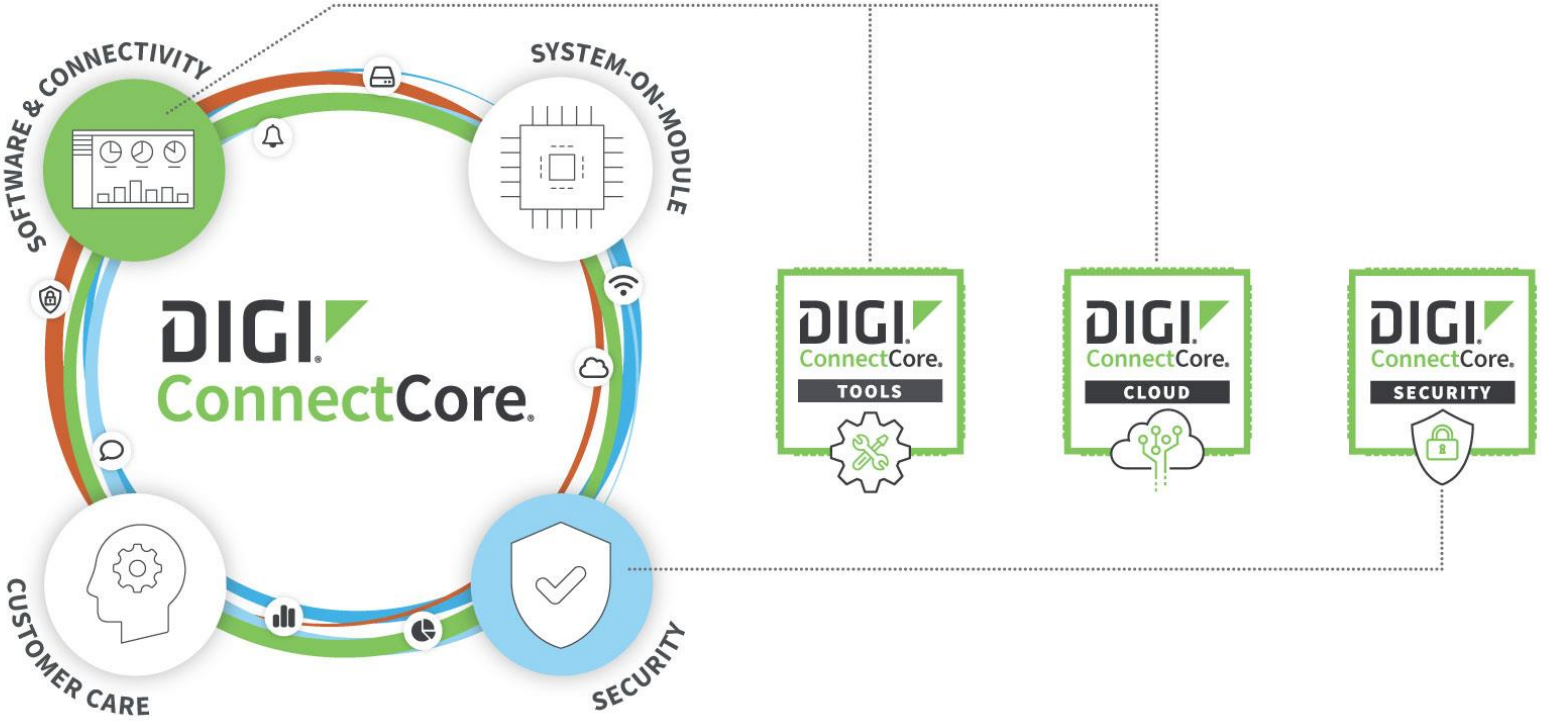
Complying with CRA leveraging Digi Security Building Blocks (IV)

PART II	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(1)	Manufacturers shall draw up a software bill of materials in a commonly used and machine-readable format	N/A	✓ Custom SBOM creation	N/A	✓ DEY SBOM
(2)	Manufacturers shall address and remediate vulnerabilities without delay	N/A	✓ meta-digi-security, consulting & support	✓ Secure remote OTA software updates, templates	✓ DEY regular releases
(3)	Manufacturers shall apply effective and regular tests and reviews of the security of the product	N/A	✓ Custom SBOM scans	✓ Digi RM Vulnerability Patch Policy	✓ DEY Patch Policy
(4)	Manufacturers shall share and publicly disclose information about fixed vulnerabilities	N/A	✓ Security Services overall	✓ Digi Security Center	✓ Digi Security Center
(5)	Manufacturers shall put in place and enforce a policy on coordinated vulnerability disclosure	N/A	N/A	✓ Digi RM Vulnerability Patch Policy, Digi Security Center	✓ DEY Patch Policy, Digi Embedded GitHub, Digi Security Center
(6)	Manufacturers shall facilitate the sharing of information about potential vulnerabilities including by providing a contact address for the reporting of the vulnerabilities discovered	N/A	N/A	✓ Digi security form	✓ Digi security form

Complying with CRA leveraging Digi Security Building Blocks (V)

PART II	DESCRIPTION	DIGI TRUSTFENCE	DIGI CONNECTCORE SECURITY SERVICES	DIGI CONNECTCORE CLOUD SERVICES	DIGI EMBEDDED YOCTO
(7)	Manufacturers shall provide for mechanisms to securely distribute updates to ensure that vulnerabilities are fixed or mitigated in a timely manner	✓ Secure software update	N/A	✓ Secure remote OTA software updates, templates, TLS, certificate-based authentication & encryption	N/A
(8)	Manufacturers shall ensure that, where security updates are available, they are disseminated without delay and, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken	N/A	N/A	✓ Secure remote OTA software updates, templates	✓ DEY Patch Policy, Digi Embedded GitHub

Digi ConnectCore SOM Solution



Security Technical Brief and free one-hour Security Session

Available Now — Digi / NXP Technical Brief:

Complying with the Cyber Resilience Act (CRA):
A Definitive Guide to Meeting the CRA Requirements

https://www.digi.com/resources/library/white-papers/complying-with-the-cyber-resilience-act-cra-wp

Get ahead of the Cyber Resilience Act with a free 1-hour consultation from Digi security experts.

Request your session here:
https://hello.digi.com/free-security-consultation

Any questions?

Many thanks!