The Cyber Resilience Act (CRA)— A Paradigm Shift

Technology Presentation

March 2026

01

Market context

Cybersecurity regulations: a turning point for manufacturers

Cyberattacks are exploding, connected devices are the epicenter

Key figures (2025)

Ransomware costs will reach $57 billion annually

A ransomware attack will strike a consumer or business every 2 seconds by 2031

IoT malware is up 37% YoY

Why connected devices remain the weakest link

Network level protections

- Encryption of connections
- Authentication in networks
  - ☑ Must become a common practice
  - ☒ But not enough to protect the device itself

Device-level vulnerabilities

- Inappropriate device configuration
- Weakness in the access control mechanisms on the device (e.g., default password)
- SW bugs in communication stack, OS, or application SW, leading to undefined device behavior
- Lack of verification on executed FW/SW
- Unpatched vulnerabilities

- Device and service unavailability
- Installation of malicious code
- Leakage of authentication keys
- Data eavesdropping
- etc.

Security incidents extend their impact way beyond individual equipment

Notable case:

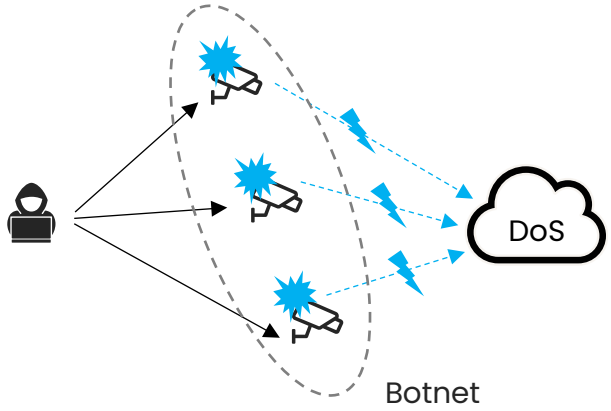
- The largest attack to date (Mirai malware) turned networked devices running Linux (IP cameras and home routers) into remotely controlled bots
- The botnet was used to execute the worst, large-scale distributed denial of service attack (DDOS) against Internet
- As a result, several websites went offline (GitHub, Twitter, Netflix, etc.)

Even low-cost consumer devices can be weaponized to disrupt global services

Business impact:

- Attacks now target industrial and critical infrastructures
- Reputational damage, service outages, and financial loss are common outcomes

➔ ***CRA mandates proactive security to prevent systemic risk***



02

What CRA is and why it matters

CRA: a turning point for Industrial IoT security in Europe

"The industry had more than 20 years to fix this problem. Now we have to step in."

– EU Policymaker

Cyber Resilience Act

- Applies to digital products in the EU market regardless of the country of origin
- Mandates addressing Essential Cybersecurity Requirements (ECRs) proportional to the risk
- Enforces conformity assessment (self-declaration or third party)
- Includes post-market obligations (vulnerability handling, mitigation measures)

Other regulations:

- RED (Radio Equipment Directive): Starting December 2027, the Cyber Resilience Act (CRA) will replace RED's cybersecurity provisions (Articles 3.3 d/e/f), introducing broader security requirements and more extensive, lifecycle-based testing for all connected products.
- US Cyber Trust Mark, UK PSTI: similar trends globally.

➔ **CRA** will set the benchmark for manufacturers' security implementation.

CRA scope and implementation: what it really covers 1/2

What counts as a “Product” under CRA

- Product handling data in binary format at a basic level
- Any hardware capable of processing, storing, or transmitting digital data
- Computer code, compiled or as source code

With direct or indirect, logical or physical connection to other products or networks.

Applies to:

- **Products** placed on the **EU market** from **Dec 11, 2027**
- **Existing (legacy) products** that continue to be **sold** on **the EU market, distributed, or made available from Dec 11, 2027**

Sector-specific exceptions:

- CRA doesn’t apply to products and systems on already regulated markets with equivalent requirements: Medical, Aeronautics, Automotive, Civil aviation, Maritime products and systems

CRA avoids overlap with existing vertical cybersecurity regulations

CRA applies to both final products and internal components

Even if shipped without pre-installed firmware, NXP digital components are considered “products with digital elements” under the CRA.

CRA scope and implementation: what it really covers 2/2

Key requirements for market access

- Security-by-design and Security-by-default
- Conformity assessment
- Vulnerability handling and security updates when applicable
- Incident reporting and lifecycle accountability

CE marking

- CRA compliance is mandatory for market access in the EU post 2027
- Products must bear the CE mark to indicate CRA compliance
- Non-compliance penalty: €15 million or 2.5% of global annual turnover, whichever is higher

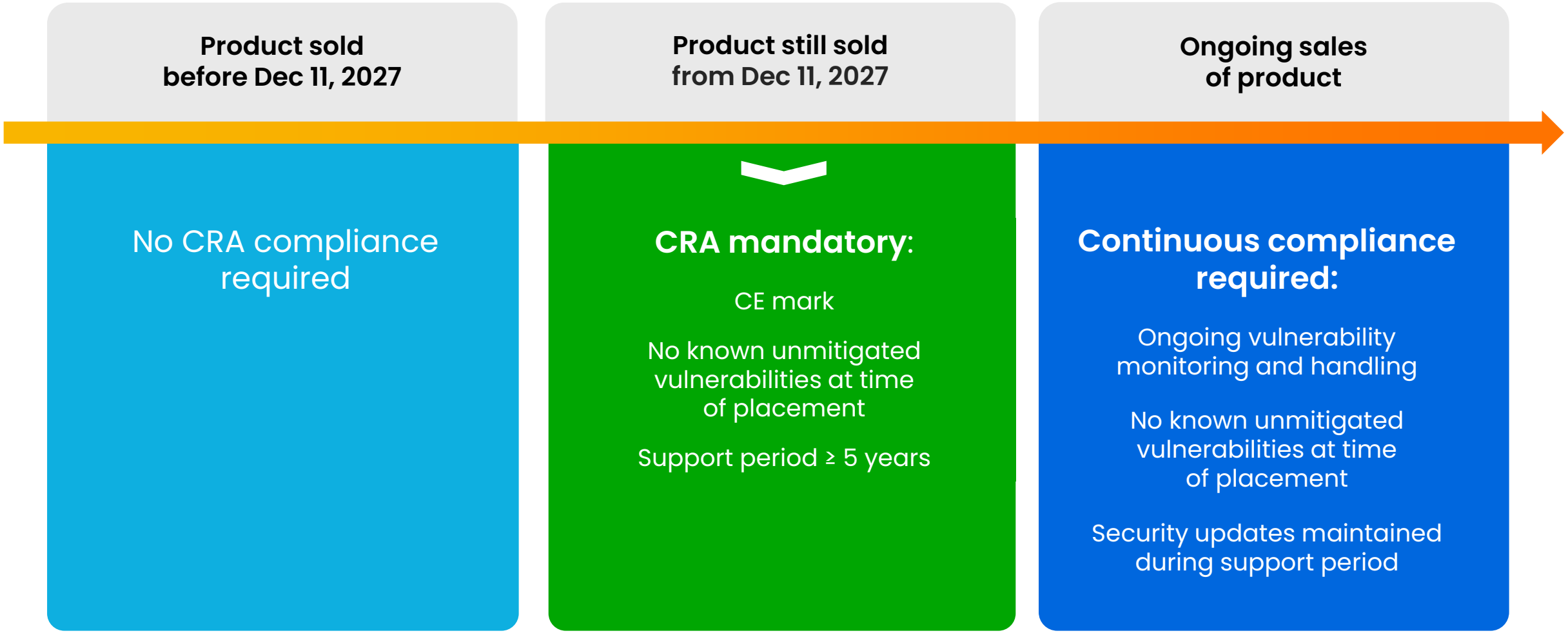
CRA applies to both final products and internal components

Even if shipped without pre-installed firmware, NXP digital components are considered “products with digital elements” under the CRA.

CRA timeline: **next milestones**

The CRA introduces a clear timeline for compliance. OEMs must anticipate which products will be placed on the EU market after December 11, 2027, and ensure those products will meet CRA requirements.

The case of legacy products



Navigating global cybersecurity regulations

What should manufacturers focus on

The OEM dilemma*: "There are so many regulations across so many regions. How do I know which one to follow to stay compliant without wasting time and money?"*

- **CRA essential requirements**: EU binding regulation, strong foundation for global compliance
- **ETSI EN 303 645**: Consumer IoT baseline (Europe, Asia)
- **IEC 62443**: Industrial control systems and OT security
- **ISO/SAE 21434**: Automotive cybersecurity requirements

➔ By aligning your products with these standards, you address approximately 90% of the global regulatory expectations for connected products.

Strategic recommendation

Start with the CRA, which provides a strong foundation to address other standards, and perform gap analysis for other standards.

Disclaimer: This recommendation is a strategic guideline, not a one-size-fits-all solution. Each manufacturer must conduct their own risk assessment and regulatory analysis based on their product type, target markets, and business model.

Navigating CRA to minimize time, cost, and complexity

CRA is mandatory, but with the right approach, OEMs can limit time, cost, and supply chain risk

Avoid delays in product launches	Limit long-term compliance cost	Secure the supply chain	Global market access	Reduce legal and operational uncertainty
Plan CRA early	Structure internal processes	Choose CRA-ready suppliers	Leverage CRA for global compliance	Document early and structure compliance evidence
Prevent redesign and bottlenecks	Avoid ad-hoc fixes	Reduce time and effort to build CRA technical file	Streamline access to international markets	Avoid penalties and recalls

03

CRA compliance made simple

From risk to conformity

A technology agnostic approach: CRA sets device security principles without specifying ‘how’

CRA ECRs **cover:**

- Product configuration
- Product authentication
- Access to product
- Data protection
- Product monitoring and Cyber State Awareness
- Vulnerability fix and product update
- Reduction of incidents’ impact and product availability

CRA **doesn’t specify:**

Level of security

Level of protections must reflect the level of risks, depending on product type, use case, and application

Functional requirements

Cryptographic algorithms, protocols, PKI, X.509 certificate format, etc.

Technological implementations

Security hardware, software, etc.

CRA require a security process beyond device capabilities, leading to deep transformation of organizations

Two layers of CRA requirements

Essential cybersecurity requirements (product-level)

Functional security requirements for products, to provide means to:

- minimize exposure and risk
- manage vulnerabilities
- minimize impact of vulnerabilities (Part I of Annex I)

Company requirements (process-level)

Organizational practices to ensure lifecycle security

- **assess** risks
- **document** (requirements, design, SBoM, …)
- **educate and inform** customers
- **collect** information on vulnerabilities
- **report and respond** to incidents (Part II of Annex I)
- **securely store** CRA compliance information

CRA conformance process: from legal requirements to real-world execution

CRA compliance is a structured process covering design, documentation, and lifecycle obligations. Follow these steps to ensure readiness for CE marking and avoid costly delays.

1

Conduct cybersecurity risk assessment

- Identify assets, threats, and vulnerabilities
- Document risks and mitigation measures
- Maintain SBOM and security records

2

Determine product classification and proof mechanism

- Map your product to CRA classes.
- Select the appropriate conformity module

3

Implement security measures

- Apply technical and organizational controls
- Define update and vulnerability management policies for lifecycle security

4

Prepare technical documentation

- Compile a complete technical file: design details, risk analysis, security controls, test results, and evidence of CRA compliance

5

Conformity declaration and CE marking

- Complete the EU Declaration of Conformity
- Affix the CE mark
- Ensure readiness for audits and market surveillance

Market surveillance and post-market obligations

- Maintain documentation for product lifecycle
- Monitor vulnerabilities, apply patches, report incidents, and support corrective actions

CRA compliance is a journey, not a checkbox.

Focus on step 2: Product classes, criticality, and conformance mechanisms

Category	Default Category	Product "Class I"	Product "Class II"	Critical Products
Examples (End products and components)	**Any product not listed in Annex III and IV** **90% of the products:** • Industrial PLC • Smartphone • EV chargers • Industrial HMI • Docking station	• PKI and digital certificate issuance software • Physical and virtual network interfaces • Operating systems • Routers and modems for internet connection, switches • MCUs/MPUs, ASICs and FPGAs with security-related functionalities • Smart home virtual assistants • Internet-connected toys • Smart lock • Wearables • Password managers	• Hypervisors and container runtime systems • Firewalls, intrusion detection, and/or prevention systems • Tamper-resistant MCUs/MPUs	• Hardware devices with security boxes • Smart meter gateways within smart metering systems • Devices for advanced security purposes • Smart cards or similar devices, including secure elements
Minimum conformance mechanism	**Self-assessment**	**Harmonized standards** (ensuring CRA principles are met)	**3rd party product assessment** (product and/or process)	**Common Criteria certification by default**

Determine your product's criticality early and plan for the required proof mechanism.

This step drives design choices and compliance effort. Anticipate early to avoid delays.

CRA compliance starts with risk ownership and documented decisions

Key takeaways:

- CRA does not mandate specific technologies
- Manufacturers are fully responsible for:
  - Assessing and mitigating risks
  - Communicating residual risks to users
- Conformance classes define how compliance is demonstrated, not security levels
- Essential requirements set security objectives, not implementation details
- Implementation choices must be:
  - Risk-based
  - Documented
  - Justified

Start with a risk assessment
Map your product and process decisions to CRA objectives and leverage secure components to simplify compliance.

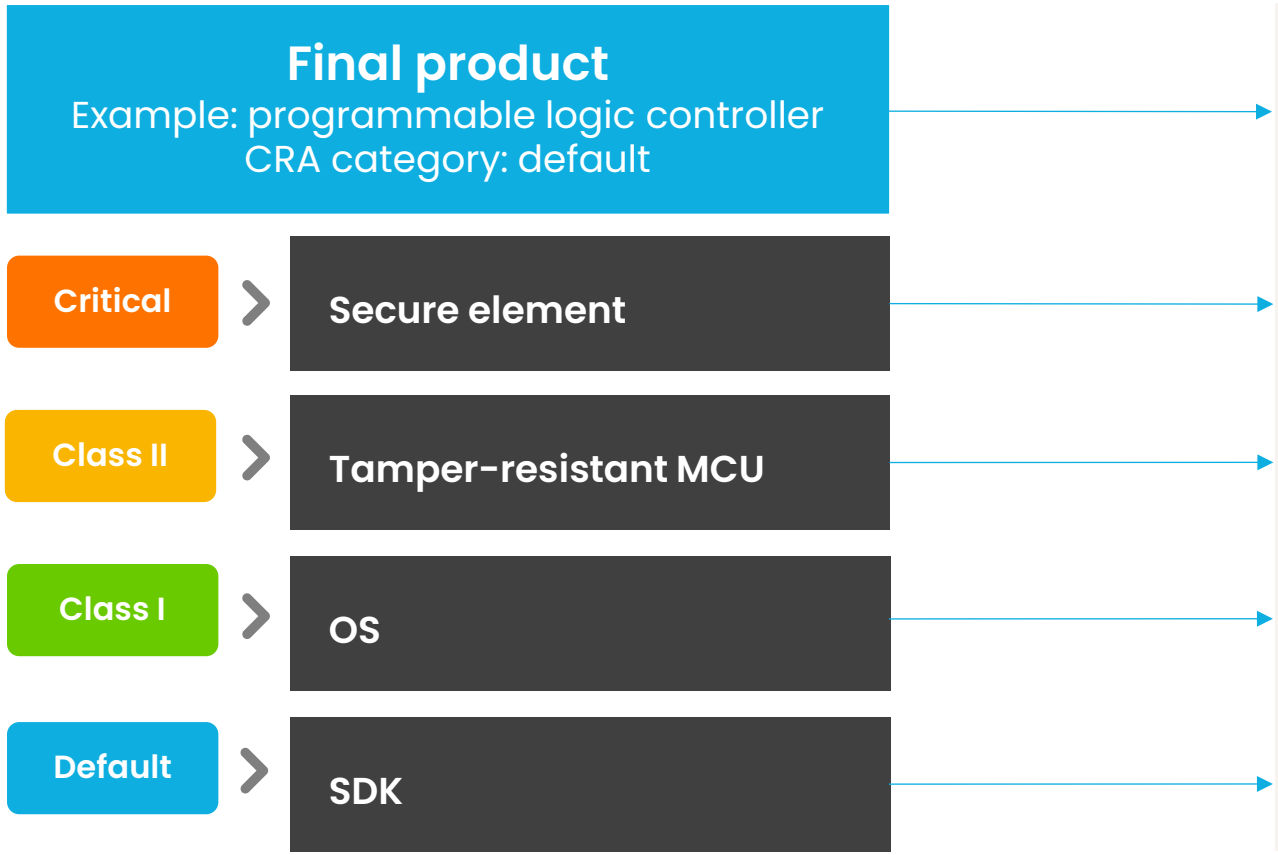
04

CRA modularity: Compliance starts at component level

CRA compliance is not just about the final product. It is about every subcomponent.

CRA modularity: aggregating compliance across subcomponents

Building the CRA technical file: from components to system



CRA technical file:

Aggregating conformity proofs from all components:

Certifications (SESIP, CC, FIPS)

SBOM and patching policies

Lifecycle security and supplier support

+

Demonstrate product-level compliance:

System-level integration of security features

End-to-end traceability

Vulnerability and update management

Traceability and supplier collaboration are essential.
Without them, compliance becomes costly and uncertain.

Components documentation: what OEMs should expect

Choosing suppliers who provide CRA-ready documentation is strategic. It reduces testing, accelerates compliance, and lowers regulatory risk.

Documents required for component certification

Supplier's responsibility, no legal obligation to share with OEM

- Risk assessment
- Vulnerability management system:
  - Patching policy and update strategy
  - Vulnerability disclosure process
- SBOM
- ECR applicability

What NXP can provide to OEM

Highly valuable to facilitate the OEM's product compliance process

- Extracts from certification's documentation
- Visibility of the residual risk, mitigations, and implementation guides
- Security certifications: harmonized standards, common specifications or European cybersecurity certification schemes
- Lifecycle support: vulnerability management strategy, incident response, end-of-support notifications

Choosing CRA-certified subcomponents is not enough.

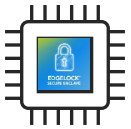
Clear, structured, and actionable documentation is key to support OEMs in building their own CRA technical file and reducing compliance friction.

Security has a lifecycle, design choices impact cost

CRA turns security upkeep into an OPEX reality

Develop with components designed to simplify compliance

- **Plan for lifecycle costs, no just upfront CAPEX** → CRA obligations (patching, vulnerability management, reporting) extend for years
- **Reuse certification evidence** (SESIP/CC/FIPS) → verify **integration** instead of re-testing functionality
- **Actionable documentation** → faster technical file
- **Lifecycle support capabilities** (secure updates, PSIRT) → helps manage risk and compliance over time
- **Security choices influence OPEX** → fewer redesigns, lower maintenance overhead, higher resilience



Selecting components designed for compliance will reduce compliance effort and long-term costs compared to retrofitting later.

Note: This is not a one-size-fits-all recommendation. The right choice depends on your risk analysis and use-case.

05

NXP’s CRA-ready solutions

Understanding the CRA is the first step. But translating it into product design decisions is where the real challenge begins.

NXP’s commitment to compliance

NXP values security and compliance highly and is dedicated to supporting your efforts to meet regulatory requirements.

Full compliance commitment

NXP commits to compliance with all applicable laws and regulations, including the Cyber Resilience Act.

Active CRA preparation

CRA enforcement starts December 11, 2027. NXP is actively preparing and monitoring evolving requirements to ensure compliance.

Clear compliance statements

NXP will provide clear statements on how each product family meets CRA classes.

CE mark assurance

from CRA applicability date, all NXP products sold in Europe will attain the CE Mark.

Proven expertise

Experience with similar requirements in medical, automotive, and industrial domains, supported by secure development processes aligned with IEC 81001-5-1, IEC 62443-4-1, ISO 21434.

Standards leadership

Active participation in CENELEC, ETSI, GlobalPlatform, Auto-ISAC, Matter, and more ensures NXP stays ahead of CRA implementation and maintains best-in-class alignment.

NXP's security solutions for CRA compliance: **security-by-design, made simple**

EdgeLock Secure Enclave (integrated on MCU/MPUs), EdgeLock Secure Elements and Authenticators

Hardware-based roots of trust and isolated execution environment for key security functions. This helps demonstrate security robustness and meet CRA requirements for vulnerability management and resilience.

Security functions on-chip with EdgeLock technology, EdgeLock 2GO services, secure provisioning tools/SDK

Extensive 'toolbox' to implement and activate product security capabilities and countermeasures as required by regulators

EdgeLock Assurance program for in-the field compliance maintenance

Procurement of secure components, with NXP Security Maturity Process and chip security certifications (SESIP1 – EN17927), providing 'Security-by-Design' at component level, independent 3rd party assessment and Product Security Incident Response (PSIRT) to handle potential vulnerabilities of released devices

From entry-level to high-assurance use cases, aligned with CRA risk-based approach

nxp.com/security

EdgeLock hardware

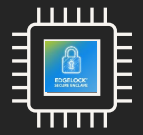
EdgeLock 2GO

Security functions available on NXP products map to regulation requirements

Required security capability (regulations)	Supporting security functions by NXP solutions[1]
Product configuration	Device lifecycle management Secure SW and credential Install Secure boot, secure update
Product authentication	Identification and authentication, attestation Secure key storage/management
Access to product	Secure debug, secure connect Secure key storage/management Crypto services for access control
Data protection	Data encryption/authentication Tamper detection, tamper resistance Secure key storage/management Privileged access to data, secure connect
Product monitoring and Cyber State Awareness	Authentication Device (runtime) attestation Secure event audit/logging
Vulnerability fix and product update	Secure update Secure key storage/management
Reduction of incidents' impact Product availability	Tamper/anomaly detection SW/data/processing isolation Damage control and device recovery Secure key storage/management

1. Please check NXP product datasheets/security manual for availability of specific security functions

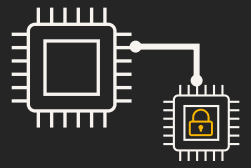
NXP advanced security technologies, made for resilience in a dynamic cybersecurity landscape



EdgeLock Secure Enclave

Dedicated security unit integrated in NXP MCU/MPU[1]

- ✓ Enhanced isolation for protection of critical security functions required by regulations
- ✓ Advanced capabilities for device monitoring and availability protection
- ✓ Protection of sensitive data and credentials
- ✓ Available on latest NXP MCU/MPUs



EdgeLock SE05x/A30

Secure elements and secure authenticators

- ✓ Secure vault for credentials with protection against SW and advanced HW attacks
- ✓ Certified Common Criteria EAL6+, FIPS
- ✓ Optional personalization with custom credentials injected at NXP manufacturing
- ✓ Can be plugged to any type of ASIC or processor
- ✓ OTA secure applet update (SE051)

EdgeLock 2GO

NXP cloud services for credential management

- ✓ Easy deployment of Root of Trust credentials on devices
- ✓ Management of credentials over-the-air and throughout device lifecycle
- ✓ Native integration on EdgeLock Secure Enclave, Secure Elements and Secure Authenticators
- ✓ Supports CRA post-market obligations (updates, vulnerability handling, revocation)

Simplify CRA compliance and strengthen resilience with integrated hardware, secure components, and lifecycle services.

Note: Please check NXP product datasheets/security manual for more info

NXP support OEM's compliance by mapping NXP security features to CRA requirements

Application note

Ease CRA compliance with **MCX N**

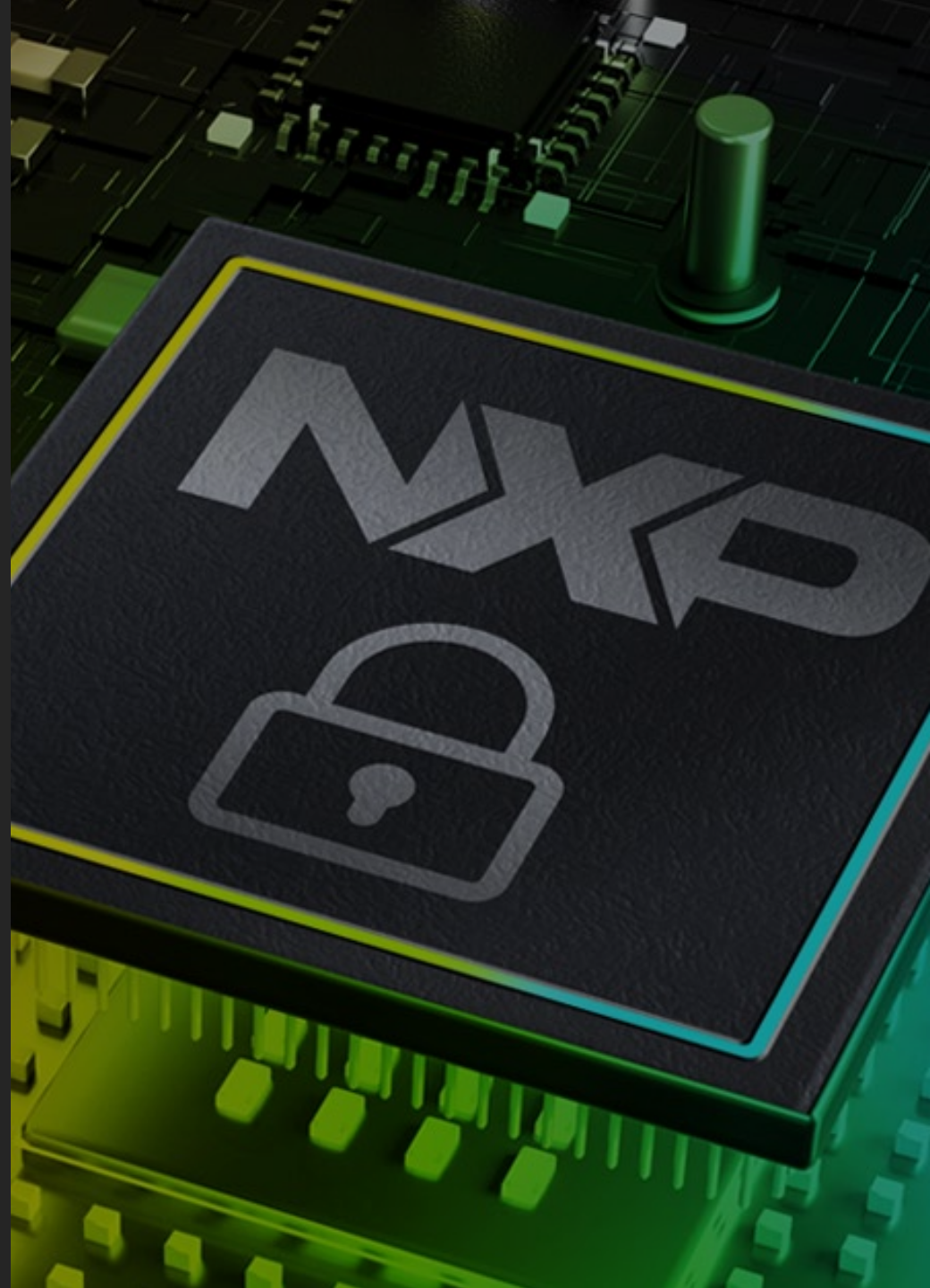
Application note

Ease CRA compliance with **i.MX 93**

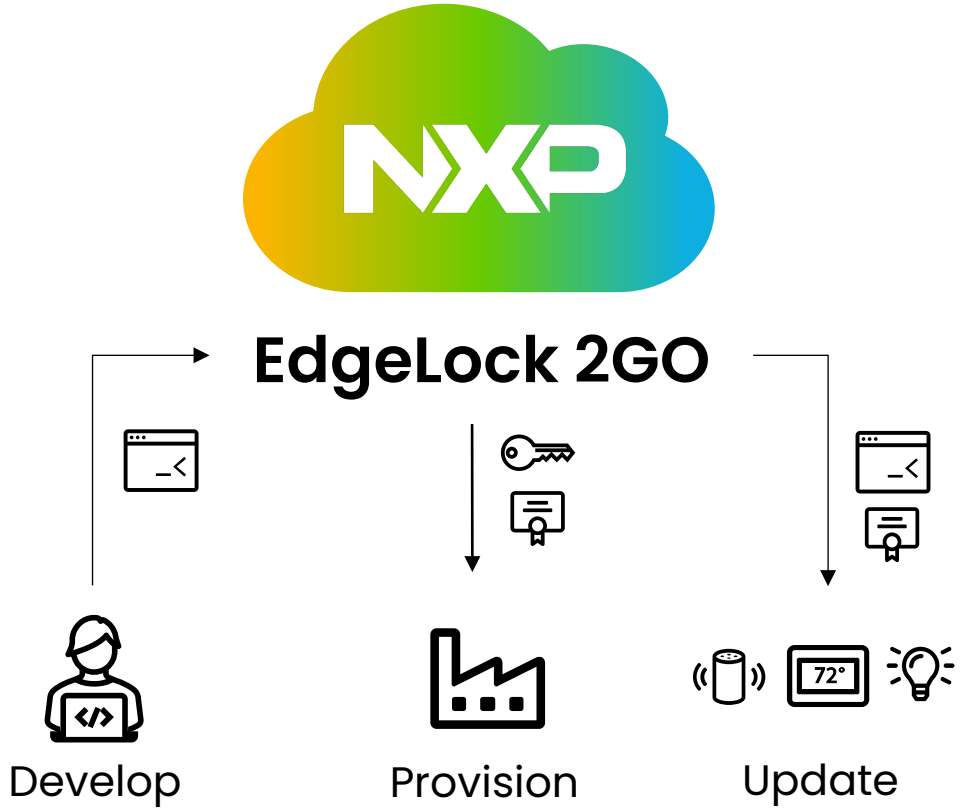
Application note

Ease CRA compliance with **EdgeLock® Discrete Portfolio**

nxp.com/CRA



The NXP service for protecting IoT devices



www.edgelock2go.com

EdgeLock 2GO simplifies CRA compliance

- ✓ **Enables security features** required by the CRA
- ✓ **Reduces attack surface** throughout the entire product lifecycle
- ✓ **Supports fast CRA compliance** with a proven, scalable service

Secure OTA update

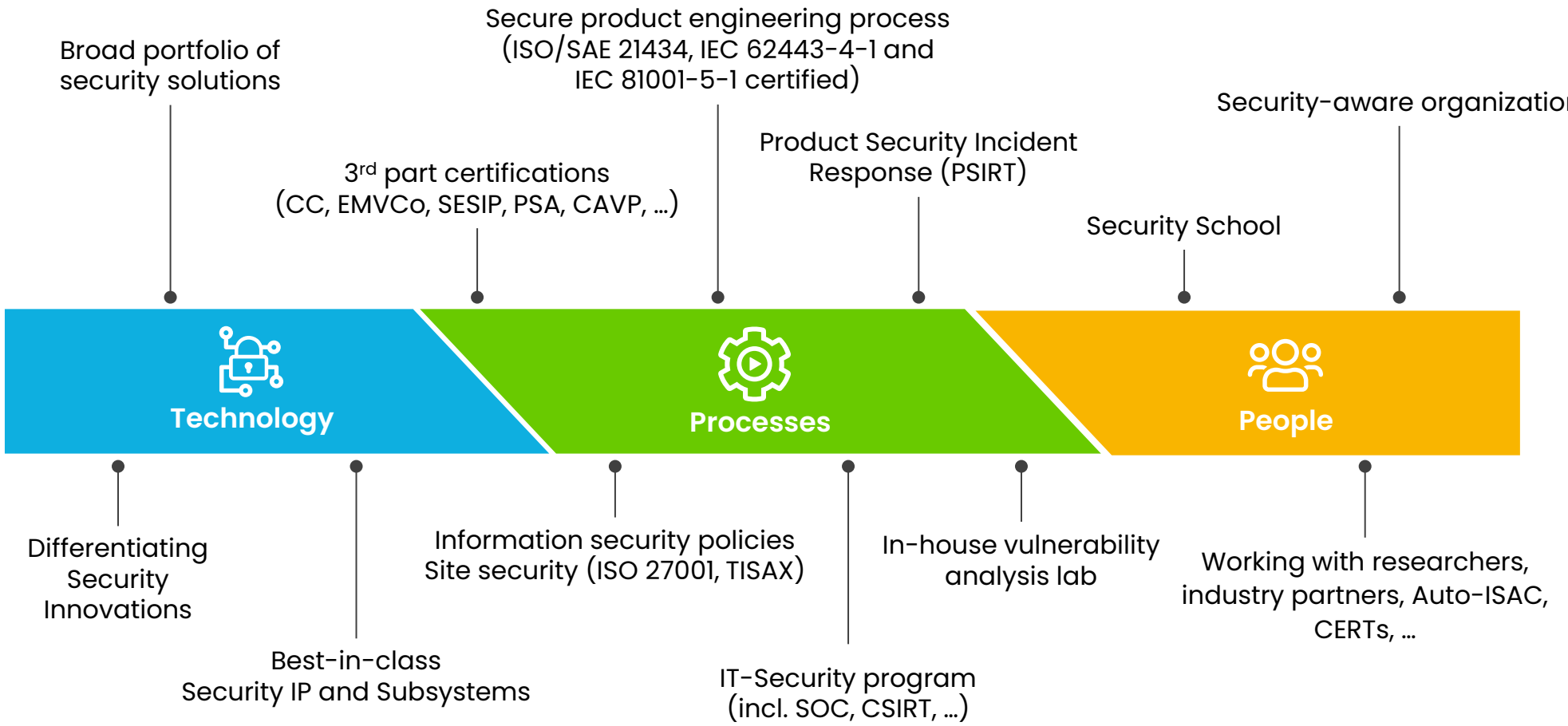
Secure code signing

Secure certificate and key management

NXP’s product security program

A holistic approach to product (cyber)security – aligned with industry standards & best-practices

20+ years in the security industry



Product Security Incident Response Team (PSIRT)

Manages product security incidents

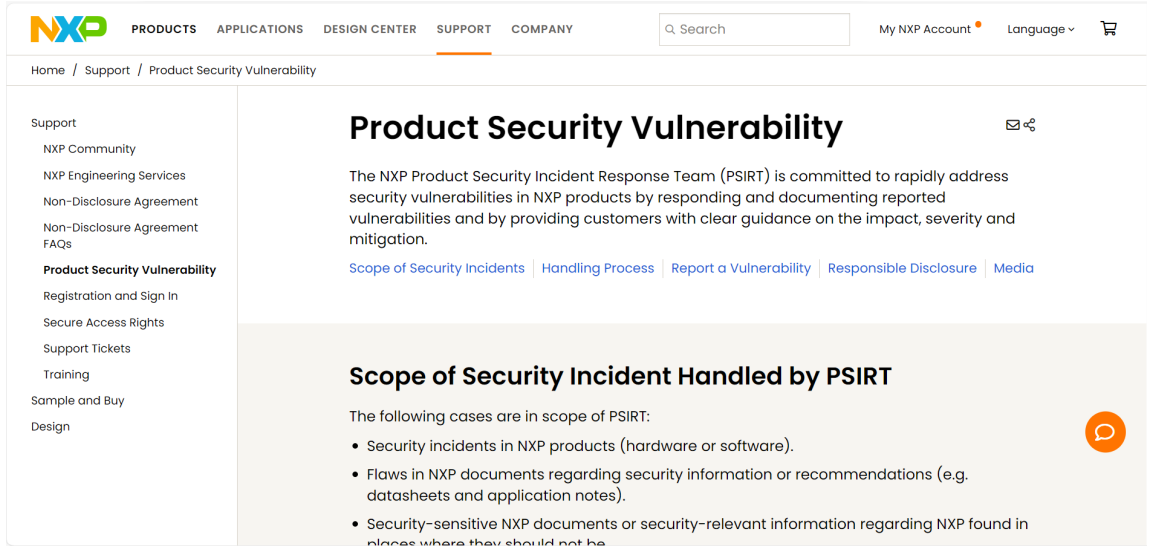
- Global across products, markets, regions
- Established in 2008 with a dedicated global team

Committed to coordinated / responsible disclosure

- In alignment with the security community, including customers, partners, Auto-ISAC, CERTs
- Plan to meet all CRA requirements

Key success factors

- The Product Security Incident Response Process (PSIRP) is IEC-62443-4-1 and TUV-SUV-ISO21434 certified
- Timely sharing of information according to disclosure guidelines
- Continuous improvement, e.g., evaluate and benchmark against Auto-ISAC's best practice guide for incidence response



Web site: www.nxp.com/psirt Contact: psirt@nxp.com

Cyber Resilience Act (CRA):

NXP is ready, and ready to support you

Trusted CRA guidance

NXP as trusted advisor providing **clear and practical support** for your CRA compliance path

Advanced security technology

Scalable, embedded security to accelerate your product compliance

Secure deployment and maintenance

Security services for secure deployment and long-term resilience to ensure your ongoing CRA compliance

nxp.com/CRA

nxp.com