/IOTCONNECT™

Security and Compliance

A practical guide to navigating the global IoT regulatory landscape with zero-trust security

Softweb Solutions Inc. | An Avnet Company

TABLE OF CONTENTS

04 Executive summary

05 The global regulatory landscape

08 /IOTCONNECT™ security architecture

11 Shared responsibility model

13 Regulatory compliance mapping

15 SBOM strategy

16 Compliance-enabling architecture advantages

18 Industry-specific compliance

19 Platform evolution: Aligned to regulatory milestones

20 Key takeaways for decision-makers

21 Regulation quick reference

22 References

24 About us

EU CRA

UK PSTI

IEC 62443

US Cyber Trust Mark

CISA SBOM

ETSI EN 303 645

Executive summary

The rules around IoT security have changed dramatically. Laws like the EU Cyber Resilience Act (CRA)[1], the US Cyber Trust Mark[4], the UK PSTI Act[3], and new SBOM requirements from CISA[8] collectively signal that IoT security is no longer optional. It's required if you want to sell your products.

/IOTCONNECT™, a secure cloud-based platform for building end-to-end IoT solutions, addresses such security and compliance concerns. With integrated security features like certificate management, zero-trust device identity, encrypted communications, and compliance-ready audit trails, the platform provides the foundation you need to secure the IoT ecosystem.

1. The global regulatory landscape

1.1 EU Cyber Resilience Act (CRA)

Regulation: EU 2024/2847[1] | **Mandatory**

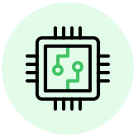
Status: In effect since December 10, 2024. Main requirements kick in on December 11, 2027. Vulnerability reporting starts September 11, 2026.

The CRA sets out strict cybersecurity rules for every “product with digital elements” sold in the EU. No matter where it’s made.

Scope and classification

Default category:
Covers products like sensors, smart home devices, and general IoT products. These can be self-assessed by the manufacturer.

Important products (Annex III):
Includes items like firewalls and industrial gateways. These need to be assessed by a third party.



Critical products (Annex IV):
Covers devices like HSMs (Hardware Security Modules) and smart meter gateways. These must undergo a mandatory third-party assessment.

The Implementing Regulation (EU) 2025/2392[2] provides more details about how products are categorized.

Essential requirements and vulnerability handling

Products must be secure by default, use encryption for data at rest and in transit, minimize possible attack surfaces, and support regular security updates. Manufacturers are also required to report any actively exploited vulnerabilities to ENISA[18] within 24 hours.

Key dates	Milestones
Dec 10, 2024	CRA comes into force
Sep 11, 2026	Vulnerability reporting requirements will begin
Dec 11, 2027	Full compliance will become mandatory

Penalties for non-compliance can be heavy:
up to €15 million or 2.5% of the company's global annual turnover.

1.2 EU Radio Equipment Directive (RED)

Status: Cybersecurity rules have been in effect since August 1, 2025. The harmonized standards (EN 18031)[5] were published in January 2025.

1.3 UK PSTI Act

Status: Active since April 29, 2024.

Three mandatory requirements: No default passwords, a clear vulnerability disclosure policy, and transparency about security updates.

Penalties: Fines up to £10 million or 4% of worldwide revenue.

Standard basis: Based on ETSI EN 303 645.

1.4 US Cyber Trust Mark Program

Status: Launched on January 7, 2025[4]. Will be mandatory for US government IoT purchases starting January 2027.

Standards basis: Built on NIST IR 8425[9]

1.5 ETSI EN 303 645

Version: 3.1.3[6] with 13 provisions.

Referenced by: UK PSTI, Singapore CLS[11], Japan JC-STAR[10], EU CRA, and US NIST[9]

1.6 IEC 62443

Focus: The main security standard for industrial IoT and operational technology (OT)[7].

Security levels: Ranges from SL 1 to SL 4.

1.7 US SBOM requirements

Basis: CISA's 2025 Minimum Elements.[8]

Drivers: Includes EO 14028[17], the EU CRA, and South Korea's 2027 regulations.

Supported formats: CycloneDX[14], SPDX[15]

1.8 Additional regional regulations

- **Japan JC-STAR:** Four security levels, with mutual recognition alongside the UK PSTI[10]
- **Singapore CLS:** Uses a four-tier labeling system.[11]
- **China CSL Amendments:** Penalties up to RMB 10 million; also covers AI governance.[12]

2. /IOTCONNECT™ security architecture

2.1 Security pillar overview

Our security approach uses a zero-trust model and six layers:

Layer 1: Device identity

- Each device gets a unique identity using X.509 certificates and mutual TLS.
- Supports different certificate authorities (like AWS IoT CA, private CAs, or enterprise CAs).
- Works with secure hardware like TPMs or HSMs.

Layer 2: Certificate lifecycle

- Certificates are provisioned automatically and rotated based on policies using MQTT.
- Expirations are tracked by AWS IoT Device Defender.
- Certificates can be revoked immediately if needed.

Layer 3: Encryption

- All data in transit is protected with TLS 1.2 or 1.3.
- Data stored at rest is encrypted with AES-256.
- Ensures end-to-end encryption across the entire telemetry pipeline.

Layer 4: Access control

- Uses role-based access control (RBAC), multi-tenant isolation, and device whitelisting.
- Can integrate with custom identity providers.

Layer 5: Network security

- Supports MQTT/MQTTS with mandatory TLS, as well as secure HTTPS and REST APIs.
- Includes anomaly detection with AWS IoT Device Defender.

Layer 6: Audit and compliance

- Keeps detailed audit trails, including certificate rotation logs.
- Makes it easy to export data for external audits.

2.2 Platform certifications

Certification	Scope	Status
ISO 27001	Softweb Solutions maintains ISO 27001 at the organizational level. /IOTCONNECT™ is covered under this certification scope.	Current
SOC 2 Type II	Softweb Solutions also maintains SOC 2 Type II at the organizational level. /IOTCONNECT™ is covered under this certification scope.	Current
GDPR	The platform is GDPR-aligned and helps customers stay compliant with EU data protection rules.	Aligned

2.3 Certificate rotation flow

- **Policy trigger:** Rotation starts when a certificate gets older than the set period.
- **MQTT notification:** A certificate signing request (CSR) is sent to the device over its topic.
- **CSR generation:** The device creates a new key pair and CSR (this can be done in secure hardware like an HSM or TPM).
- **Certificate issuance:** The certificate authority (CA) signs the CSR and sends the new certificate back.
- **Policy transfer:** The necessary IoT policies are attached to the new certificate.
- **Activation:** The device switches to the new certificate and the old one is deactivated.
- **Audit:** Every rotation event is logged for compliance and auditing.

3. Shared responsibility model

/IOTCONNECT™ gives you the platform and tools needed for IoT security and compliance. Real-world security is a shared responsibility between the platform, the device firmware, and the hardware.

The key idea: /IOTCONNECT™ makes compliance possible by offering the right mechanisms, infrastructure, and audit trails. But it's up to device manufacturers to integrate these features and make sure their finished products are certified and fully compliant.

3.1 Responsibility matrix

Domain	/IOTCONNECT™ platform	Device firmware	Hardware
Device identity	Handles certificate provisioning, CA hierarchy, and lifecycle management	Generates CSRs, installs certificates	Provides secure key storage via TPM/HSM
OTA updates	Manages secure delivery, staged rollouts, scheduling, delta packaging, and audit trails	Validates downloads, checks installation integrity, supports rollback and boot verification	Ensures secure boot chain and flash protection
Encryption (In transit)	Enforces TLS 1.2/1.3 at the broker, manages MQTT/MQTTS connections	Implements TLS client, manages cipher suites, validates hostnames	Supports hardware crypto acceleration
Encryption (At rest)	Encrypts cloud-stored telemetry and configuration with AES-256	Encrypts local data on the device	Uses secure storage elements
Access control	Provides RBAC, multi-tenant isolation, whitelisting, and quarantine	Handles session management and credential rotation	Offers physical tamper protection
Vulnerability Management	Monitors CVEs, manages SBOMs, and provides a disclosure via security@iotconnect.io	Monitors firmware CVEs and patches components	Tracks hardware errata
Audit and compliance	Logs events, tracks certificate rotations, and generates compliance reports	Creates local audit logs and forwards events	Reports hardware security events
Input validation	Validates inputs at the API layer, enforces protocol rules	Validates at the SDK layer and parses protocols	N/A

3.2 SDK and Integration components

The /IOTCONNECT™ SDKs and reference implementations (available at www.github.com/avnet-iotconnect) are designed to help with integration. They aren't standalone products or fully compliant solutions on their own. It's up to device manufacturers to harden these components for production, handle hardware integration, and make sure their final products meet regulatory requirements.

Each maintained repository includes a SECURITY.md file with clear instructions for reporting vulnerabilities (via security@iotconnect.io), as well as details on how the repository is classified and up-to-date SBOMs for every release.

3.3 Vulnerability disclosure and response

- If you discover a security issue, you can contact us directly at security@iotconnect.io.
- We use a coordinated disclosure process: you'll get a response within 24 hours, and we prioritize triage and resolution based on how severe the issue is.
- Details on our full response process and service level agreements are outlined in the /IOTCONNECT™ Security Response Policy.

3.4 Platform lifecycle and support commitment

- /IOTCONNECT™ has a clear platform lifecycle policy published at iotconnect.io. This policy defines support tiers, Active, Maintenance, Extended, and End of Life, and sets minimum periods for security updates.
- Customers are notified in advance about any changes in support status, giving you plenty of time to plan migrations or upgrades before support ends.
- This approach fulfills UK PSTI Requirement 3 and CRA requirements for ongoing security updates.

4. Regulatory compliance mapping

4.1 How /IOTCONNECT™ meets EU CRA requirements

CRA requirement	/IOTCONNECT™ capability	Coverage
Secure-by-default	Template-based provisioning	✓ Full
No exploitable vulns at delivery	OTA firmware management	✓ Full
Authentication mechanisms	X.509 mutual TLS, per-device certificates	✓ Full
Data protection in transit	TLS 1.2/1.3 mandatory	✓ Full
Data protection at rest	AES-256 encryption	✓ Full
Minimize attack surfaces	RBAC, whitelisting, quarantine	✓ Full
DoS resilience	Cloud-native auto-scaling, DDoS protection	✓ Full
Security monitoring	Telemetry, Device Defender, audit trails	✓ Full
Security updates	OTA with staged rollout, delta, rollback	✓ Full
Vulnerability handling	Coordinated disclosure via security@iotconnect.io	✓ Full
SBOM documentation	Platform SBOM maintained; device-level ahead of CRA Dec 2027	▶ Ahead of Mandate
ENISA incident reporting	Audit trails enable rapid ID; reporting ahead of Sep 2026	▶ Ahead of Mandate

4.2 ETSI EN 303 645

All 13 provisions of the standard are fully covered[6]. Vulnerability disclosures can be submitted to security@iotconnect.io, with a guaranteed response within 24 hours.

4.3 UK PSTI & US NIST

We meet all three mandatory requirements[3] of the UK PSTI Act and address all seven criteria[9] set by US NIST.

4.4 IEC 62443

All seven foundational requirements (FR 1–7)[7] of IEC 62443 are fully met.

5. SBOM strategy

5.1 Platform-Level SBOM

/IOTCONNECT™ keeps a detailed Software Bill of Materials (SBOM) that lists all software components and dependencies on the platform. You can request the platform SBOM in standard industry formats like CycloneDX or SPDX. This meets transparency requirements from both CISA[8] and the EU CRA[1].

5.2 Device-Level SBOM (In Development)

We are actively working to stay ahead of future regulations. Upcoming features include an SBOM Ingestion API (supporting CycloneDX[14] and SPDX[15] formats), automated matching of CVEs, SBOM versioning, and tools for compliance reporting.

5.3 AI Model SBOM (ML-BOM)

Our ML-BOM documents cover every detail of our AI models, including architecture, sources of training data, optimization methods, and performance benchmarks, getting us ready for the EU AI Act's requirements.

6. Compliance-enabling architecture advantages

Certificate-first identity:

Using X.509 certificates cover several requirements at once, including UK PSTI Requirement 1, ETSI Provision 1, CRA's secure-by-default mandate, and NIST's asset identification standards.

Automated lifecycle management:

Features like certificate rotation, monitoring, and revocation help meet CRA vulnerability handling requirements and ETSI Provision 3.

OTA as compliance infrastructure:

The CRA requires security updates throughout a product's entire lifecycle, and our OTA capabilities make this possible.

Multi-cloud flexibility:

Supports AWS and Azure, and works across various protocols like MQTT, HTTPS, BLE, LoRaWAN, and 5G/LTE.

Comprehensive audit trails:

Every security event is logged, providing the evidence you need for CRA conformity, IEC 62443 audits, and SOC 2 compliance.

Competitor approach	Limitation	/IOTCONNECT™ advantage
Password-based authentication	Fails to meet PSTI, ETSI, and CRA requirements	Certificate-first approach eliminates this issue
Manual certificate management	Doesn't scale and prone to human error	Automated certificate lifecycle with policy-driven rotation
Single-cloud platforms	Vendor lock-in reduces flexibility	Consistent security across AWS and Azure (multi-cloud)
No OTA capability	Cannot deliver required security updates	Full OTA support with staged rollout, rollback, and audit
Point security solutions	Compliance evidence is fragmented	Integrated security pillar with a unified audit trail
Consumer-grade IoT	Lacks industrial-level compliance	Enterprise-grade platform with ISO 27001 and SOC 2 certified

7. Industry-specific compliance

Healthcare

Using X.509 certificates cover several requirements at once, including UK PSTI Requirement 1, ETSI Provision 1, CRA's secure-by-default mandate, and NIST's asset identification standards.

Manufacturing and industrial

We meet both IEC 62443 and CRA requirements by integrating device identity and continuous monitoring. It helps manufacturers stay compliant across regions.

Energy and utilities

Our certificate management and robust audit trails ensure compliance with both NERC CIP and CRA rules at the same time.

Retail and smart buildings

We address overlapping requirements from CRA, PSTI, and the US Cyber Trust Mark. Our integrated approach makes it easier to get certified in multiple markets without extra complexity.

8. Platform evolution: Aligned to regulatory milestones

/IOTCONNECT™ delivers capabilities ahead of the corresponding mandate.

Capability	Driver	Mandate	Platform delivery
SBOM Ingestion and Management API	CRA, CISA, EO 14028	Dec 2027	**H2 2026 — 18 months early**
Automated CVE correlation	CRA vulnerability handling	Dec 2027	**H2 2026 — 18 months early**
ENISA incident reporting	CRA Article 14	Sep 2026	**H1 2026 — 6 months early**
Third-party CA marketplace	Enterprise PKI	Dec 2027	**H2 2026 — In progress**
ML-BOM for AI transparency	EU AI Act, CRA	Aug 2027	**H1 2027 — 6 months early**
Conformity assessment docs	CRA CE, Cyber Trust Mark	Dec 2027	**H1 2027 — 12 months early**
IEC 62443 SL-2/SL-3 cert	Industrial demand	Ongoing	**H1 2027 — Proactive**
HSM/TPM integration	CRA, IEC 62443	Dec 2027	**H1 2027 — 12 months early**

/IOTCONNECT™ consistently delivers key features ahead of regulatory deadlines, helping you stay compliant with time to spare.

9. Key takeaways for decision-makers

Compliance deadlines are coming fast

The UK PSTI is already being enforced. The EU RED takes effect in August 2025, and CRA requirements kick in by December 2027.

Regulations are aligning worldwide

ETSI EN 303 645 is becoming the common standard across the UK, EU, Japan, Singapore, and the US.

Certificate-based identity is essential

Every major regulation bans default passwords—unique certificates for each device are now the norm.

OTA updates are no longer optional

The CRA requires ongoing security updates throughout a product's life. If your devices can't receive OTA updates, you won't be able to sell in the EU after December 2027.

SBOMs are quickly becoming mandatory

CISA 2025, the CRA, and South Korea's 2027 regulations all point to SBOMs as a baseline requirement.

Using a compliant platform saves money

Platforms like /IOTCONNECT™, which are already certified (ISO 27001, SOC 2, GDPR), help you inherit a strong compliance posture and reduce your overall costs.

10. Regulation quick reference

Regulation	Region	Type	Key Date	Penalties
EU CRA	EU	Mandatory	Dec 2027	€15M or 2.5% of revenue
RED Art. 3(3)	EU	Mandatory	Aug 2025	Varies
UK PSTI Act	UK	Mandatory	Active	£10M or 4% of revenue
US Cyber Trust Mark	US	Voluntary (Govt required	TBD	Procurement only
ETSI EN 303 645	Global	Standard	Current	N/A
IEC 62443	Global	Standard	Current	N/A
CISA SBOM 2025	US	Guidance	Draft	N/A
Japan JC-STAR	Japan	Cert	Active	N/A
Singapore CLS	SG	Label	Active	N/A
China CSL	China	Mandatory	Jan 2026	RMB 10M

11. References

1. **EU Cyber Resilience Act (EU 2024/2847)** — Official regulation text
https://eur-lex.europa.eu/eli/reg/2024/2847/oj

2. **EU CRA Implementing Regulation (EU 2025/2392)** — Product category descriptions
https://eur-lex.europa.eu/eli/reg_impl/2025/2392/oj

3. **UK PSTI Act 2022** — Product security guidance
https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets

4. **US Cyber Trust Mark** — FCC IoT labeling
https://www.fcc.gov/cybersecurity-certification-mark

5. **EN 18031 Series** — RED cybersecurity standards
https://www.cencenelec.eu

6. **ETSI EN 303 645 v3.1.3** — Consumer IoT security baseline
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

7. **IEC 62443 Series** — Industrial cybersecurity
https://www.iec.ch/cyber-security

8. **CISA SBOM Resources** — Minimum elements and guidance
https://www.cisa.gov/sbom

9. **NIST IR 8425** — IoT Core Baseline
https://csrc.nist.gov/publications/detail/nistir/8425/final

10. **Japan JC-STAR** — METI IoT certification
https://www.meti.go.jp/english/policy/mono_info_service/information_economy/cybersecurity/

11. **Singapore CSA CLS** — Cybersecurity Labelling
https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme

12. **China CSL 2025 Amendments** — Cybersecurity law amendments
https://www.chinalawtranslate.com/en/cybersecurity-law/

13. **EU AI Act (EU 2024/1689)** — AI regulation
https://eur-lex.europa.eu/eli/reg/2024/1689/oj

14. **CycloneDX** — OWASP SBOM standard
https://cyclonedx.org/

15. **SPDX** — Linux Foundation SBOM standard
https://spdx.dev/

16. **AWS IoT Device Defender** — IoT auditing
https://aws.amazon.com/iot-device-defender/

17. **US Executive Order 14028** — Improving cybersecurity
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

18. **ENISA** — EU cybersecurity agency
https://www.enisa.europa.eu/

19. **ISO/IEC 27001:2022** — ISMS standard
https://www.iso.org/standard/27001

20. **/IOTCONNECT™ Platform** — Softweb Solutions IoT platform
https://IOTCONNECT™.io

ABOUT /IOTCONNECT™

/IOTCONNECT™ is an enterprise-grade IoT Platform as a Service (PaaS) by Softweb Solutions, an Avnet company. It helps businesses easily connect, track, and manage all their connected devices in one secure place. Working smoothly with major cloud providers like AWS and Azure, /IOTCONNECT™ specializes in turning raw machine data into real-time alerts and clear insights. The platform makes it easy for companies to automate their everyday operations.