Addressing the EU Cyber Resilience Act (CRA)

with Integrity Security Services (OmniTrust)

EU CRA

Requirements At a Glance

What is it? An EU regulation that sets security-by-design rules for products with digital elements—hardware, software, and any remote services the manufacturer controls—across the full lifecycle. Conformity results in an EU Declaration of Conformity and CE marking; some higher-risk products also require a notified body/EU certification route. Key timing: reporting starts Sept 2026; most product obligations apply Dec 2027.

Program basics:

- **Scope: Whole product you control** — device + software + cloud/remote parts you operate.
- **Two requirement sets** — Product properties (how the product behaves) and Vulnerability handling (how you test, fix, and inform).
- **Conformity & CE —** internal control for most; "important/critical" categories may need a notified body or EU cybersecurity certificate; harmonized standards/Common Specifications show conformity.
- **Reporting & support** — report actively exploited vulns/incidents (early warning 24h; details 72h; final follow-ups); define and disclose a support period and keep security updates available long-term.

- **Secure by Design** — Build to a risk-based bar; ship with no known exploitable vulnerabilities.
- **Secure Defaults & Reset** — Ship secure settings and an easy "restore secure defaults."
- **Identity & Interface Access** — Authorize who/what can use device, app, and cloud interfaces.
- **Data Protection** — Protect confidentiality, integrity, and minimize data as designed.
- **Resilience & Logging** — Keep essentials running, avoid harming others, and log security events.
- **Updates & Support** — Secure updates, auto-install by default with opt-out; publish support period; keep updates available.
- **SBOM & Testing** — Maintain a machine-readable SBOM (top-level deps) and test regularly.
- **CVD, Contact & Advisories** — Run a coordinated vulnerability disclosure process, provide a public contact, and issue free security advisories.

OmniTrust
Formerly ISS

On the next page, we'll show how the OmniTrust Trust Lifecycle Management platform and services map to Enabling documented, audit-ready compliance across the full product lifecycle - from silicon to AI. Approaching compliance from silicon to supply chains and device ecosystems.

>

OmniTrust
Formerly ISS

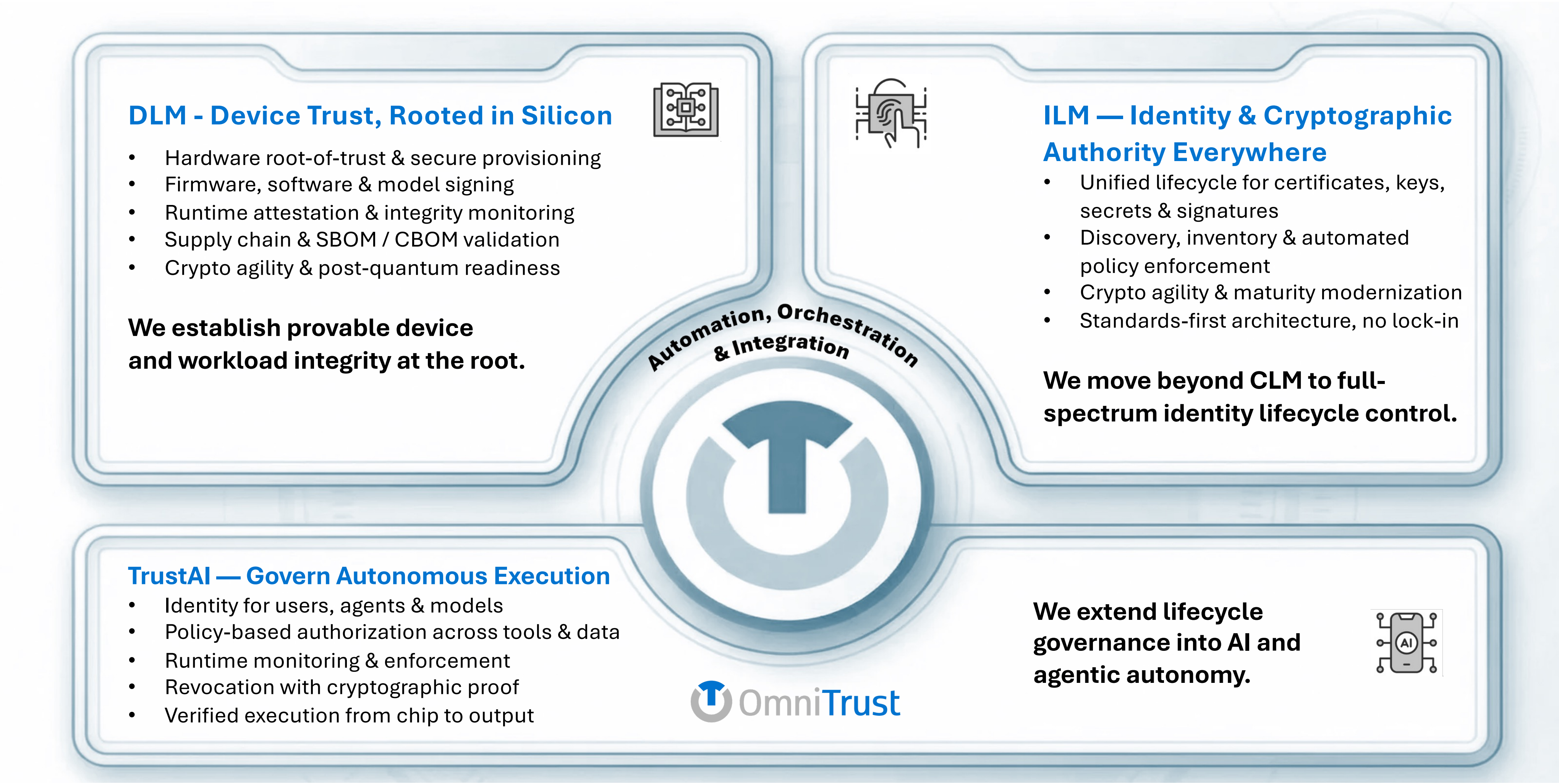
Securing What Matters for CRA from Silicon to AI

- **DLM** secures devices.
- **ILM** secures keys and certificates.
- **TrustAI** governs autonomous intelligence, from silicon to outcome

CRA requires governance across devices, identities, signing authorities, update systems, and supply chain cryptographic dependencies. It requires a holistic approach to device lifecycle security that isn't solved with a single solution like PKI, CLM, OTA, or SBOM.

User / Outcome	TrustAI
Tool / MCP	TrustAI
Agent / Interaction	TrustAI
Model / Asset	ILM + TrustAI
Runtime / Execution	TrustAI
Firmware / OS	DLM
Silicon / GPU	DLM

www.omnitrust.com



DLM - Device Trust, Rooted in Silicon

- Hardware root-of-trust & secure provisioning
- Firmware, software & model signing
- Runtime attestation & integrity monitoring
- Supply chain & SBOM / CBOM validation
- Crypto agility & post-quantum readiness

We establish provable device and workload integrity at the root.

ILM — Identity & Cryptographic Authority Everywhere

- Unified lifecycle for certificates, keys, secrets & signatures
- Discovery, inventory & automated policy enforcement
- Crypto agility & maturity modernization
- Standards-first architecture, no lock-in

We move beyond CLM to full-spectrum identity lifecycle control.

Automation, Orchestration & Integration

TrustAI — Govern Autonomous Execution

- Identity for users, agents & models
- Policy-based authorization across tools & data
- Runtime monitoring & enforcement
- Revocation with cryptographic proof
- Verified execution from chip to output

We extend lifecycle governance into AI and agentic autonomy.

OmniTrust

PQC | **EU CRA** | DORA | NIS2 | NIST CSF 2.0 | NIST SP 800-53 | NIST SP 800-57 | NIST SP 800-218 (SSDF) | Executive Order 14028 | CISA | PCI DSS 4.0
SOC 2 | ISO 27001:2022 | ISO 27400 (IoT Security) | GDPR | eIDAS 2.0 | NYDFS 23 NYCRR 500 | UK PSTI Act | SEC Cyber | SBOM / NTIA

OmniTrust

Mapping OmniTrust Trust Lifecycle Management (TLM) to EU CRA Requirements

EU CRA

			Compliance Areas							
OmniTrust TLM Platform Layer	OmniTrust Product	WHAT IT DOES	Secure by Design	Secure Defaults & Reset	Identity & Interface Access	Data Protection	Resilience & Logging	Updates & Support	SBOM & Testing	CVD, Contact & Advisories
Device Lifecycle Management	FLEX	Runtime enforcement, edge crypto, anomaly/tamper detection.	Risk-based controls at edge	Enforce secure defaults at runtime	Local allow/deny by policy	Protect code/data integrity	Tamper/health signals to logs			
	TRUST	Secure boot & code signing; hardware root of trust.	Signed integrity chain at boot	Signed rollback to known-good	Block rogue services at startup	Firmware integrity protection	Boot attestation events			
	UPDATE	Signed OTA with staging, rollback, policy control.		Policy windows & approvals	Gate updates to authorized endpoints	Encrypted, verified payloads	Update success/failure telemetry	Signed OTA; auto-install default with opt-out	Update lineage evidence	
Identity Lifecycle Management	PKI	Identity lifecycle governance for device, service, and human identities	Least-privilege identity baselines Automated revocation on compromise	Policy-driven cert profiles	Cert-gated access (devices/services)	mTLS: encryption + mutual authentication	Expiry/OCSP/CRL alerts Tamper-evident logs	Manage signer Cas Signing key lifecycle governance and custody controls	Issuance/rotation logs (evidence)	Credential revocation at scale in response to disclosed vulnerabilities
	ILM (Secrets & Keep)	Credential issuance, rotation, revocation at scale. Policy-enforced access across device, API, and cloud interfaces		Least-privilege credential policies	Credential-based access control	Rotate creds by policy	Identity event history	Push/revoke creds at scale	Credential registry	Rotation & recovery runbooks
	ILM Secrets & Keep	Hardened storage/rotation for secrets, tokens, passwords, keys.	Enforced credential rotation policies	Centralized secure storage	Token-scoped access control	Encrypt secrets at rest	Misuse/rotation alerts	Feed secrets to orchestrations	Key-custody records	Password/API-key guidance
Cryptographic Discovery, Inventory & Orchestration (ILM))	ILM Discovery	Discover crypto assets; build SBOM/CBOM; surface risks/owners.		Flag weak configs & drift	Find exposed/legacy services	Inventory crypto assets and map dependencies to support SBOMs	Crypto-misuse alerts	Cryptographic asset discovery to support accurate SBOM	SBOM (top-level), test evidence	Intake & response support
	CUMULUS Trust Control Plane	Governance dashboards; CE marking support artifacts and audit-ready exports.		Baseline compliance views		Posture dashboards	Compliance alerts	Support-period & update evidence	Audit-ready exports	Comms templates Coordinated vulnerability disclosure workflow support
Consulting & Expert Services & AI Accelerators		Architecture, readiness, validation, drills, training.	Threat modeling (TARA), crypto architecture validation /risk-based design evidence.	Default-hardening & secure decommissioning	Interface threat-model & hardening	Crypto design reviews	Incident & logging Evidence retention aligned to CRA reporting timelines	Update/auto-install program & EOS comms	SBOM/CVD process setup & training	Advisory templates; comms & contact setup