What is the number one security solution to prevent cyber attacks?

Secure-by-design architecture

(memory-safe, least-privilege systems)

Why this is #1

Most successful cyber attacks exploit **fundamental design weaknesses** and **unavoidable programming errors**. Secure-by-design systems prevent entire classes of attacks **before they exist**. In practice, this means:

Memory-safe execution

Eliminates buffer overflows, use-after-free, etc.

Strong isolation & compartmen-talisation

Limits blast radius of bugs

Least privilege by default

Prevents escalation of privilege

Verified boot & trusted roots

Prevents persistent compromise

Why software security tools alone are not enough

Firewalls, antivirus, IDS, patching, and monitoring are important - but they are **reactive.** They assume vulnerabilities will exist and try to detect or mitigate them **after the fact**.

Secure-by-design:

- Aligns with modern regulation (CRA, NIST, ENISA)
- Removes entire attack vectors
- Makes exploitation economically unattractive
- Reduces attack surface permanently

The most effective way to prevent cyber attacks is to build systems that are secure by design - using memory-safe, isolated, least-privilege architectures that prevent vulnerabilities from becoming exploits.

ICENI™ – Your CRA Business Enabler

CRA Core Principle & Requirement	ICENI Secure-by-Design Mapping
1. Security by Design & by Default Products must be designed and produced to ensure cybersecurity and minimize vulnerabilities from the outset.	• Memory-safe execution prevents entire classes of vulnerabilities (e.g., buffer overflows, use-after-free). • Least-privilege and compartmentalisation ensure secure defaults. • Attack surface is reduced at design time, not patched later. ✅ **Direct compliance with CRA secure-by-design requirements**
2. Vulnerability Prevention & Exploit Mitigation Products must prevent known exploitable vulnerabilities and limit the impact of incidents.	• Memory safety eliminates the most common root cause of critical exploits. • Isolation ensures a single bug cannot compromise the whole system. • No escalation of privilege is possible by design. ✅ **Meets CRA requirements for vulnerability reduction**
3. Protection Against Unauthorized Access Products must protect against unauthorized access, modification, or interference.	• Strong isolation boundaries prevent lateral movement. • Least-privilege execution blocks unauthorized operations. • Secure boot ensures only authenticated software runs. ✅ **Directly addresses CRA access control and integrity**

ICENI – Your CRA Business Enabler

CRA Core Principle & Requirement	ICENI Secure-by-Design Mapping
4. Secure Development & Architecture Transparency Manufacturers must demonstrate secure software development and system architecture understanding.	• Explicit compartment boundaries define trust relationships. • Architecture is analyzable and auditable. • Security properties are system-enforced, not developer-dependent. ✅ **Supports CRA conformity assessment and documentation**
5. Risk Assessment & Threat Modeling Products must undergo cybersecurity risk assessment and mitigation.	• System interactions are explicitly defined and analyzable. • Blast radius of failures is known and measurable. • Threats are structurally constrained by architecture. ✅ **Enables objective, repeatable CRA risk assessments**
6. SBOM & Supply Chain Security Manufacturers must document software components (SBOM) and manage third-party risks.	• Clear software structure simplifies SBOM creation. • Third-party components are isolated, limiting their risk. • Open-source vulnerabilities cannot compromise the whole system. ✅ **Supports CRA supply-chain and SBOM obligations**
7. Incident Impact Limitation Products must limit the impact of cybersecurity incidents.	• Compartmentalisation prevents system-wide compromise. • Memory-safe execution blocks reliable exploitation. • Failures are contained and recoverable. ✅ **Meets CRA incident containment expectations**

ICENI CHERIoT CORE

PROJECT: PRODUCT SECURITY & CYBER RISK MITIGATION
INTEL: CYBER RESILIENCE ACT (CRA) COMPLIANCE
ENFORCEMENT: CHERIoT TECHNOLOGY

01. PRODUCT SECURITY COMPLIANCE

CHERIoT technology enforces compliance by:

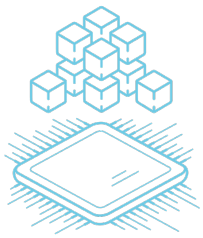
INTEGRITY
Secure boot and secure initial device configuration.

SAFEBOXES
Safeboxes for secure storage of cryptographic keys.

IMPLEMENTATION
Secure and fine-grained compartmentalisation.

02. MINIMISING CYBERSECURITY RISK

PROTOCOL	FUNCTIONAL IMPACT
MITIGATION	Mitigates attacks caused by memory-safety bugs.
REDUCTION	Reduces the overall attack surface.
ISOLATION	Isolates bugs in compartments to prevent system-wide exploits.
PREVENTION	Prevents escalation of privilege - by design.
RESILIENCE	Limits the blast radius of any potential breach.



03. RISK ASSESSMENT, AUDITABILITY & GOVERNANCE

CHERIoT technology and toolchain further support compliance by:

Comprehensive Risk Assessment

ANALYSIS
Audit toolchain analyses every interaction in the system.

IDENTIFICATION
Identifies security gaps and analyses breach impact.

VULNERABILITY_BARRIER
Closes potential loopholes created by zero-days in third-party open-source

Software Transparency & Governance

ARCH_MAPPING
Analyses software structure and software system architecture

SBOM_SUPPORT
Supports creation of the Software Bill of Materials (SBOM)

ENFORCEMENT
Defines and enforces appropriate security policies.