SoftServe

Protect Your Connected Devices from Hidden Risks

19 billion IoT devices are active today, twice as many as five years ago. At the same time, the EU Cyber Resilience Act introduces strict compliance deadlines starting September 2026 for any connected device sold in Europe.

THE PROBLEM

Embedded and IoT devices cannot support traditional security tools due to limited resources. Yet they are widely connected, tightly regulated, and a frequent target for attackers.

WHAT IS AT STAKE

One vulnerable device can expose your entire system. The impact goes beyond a breach — fines, mandatory disclosure, and lasting reputational harm follow.
In healthcare, the majority of connected medical devices carry known critical vulnerabilities.

WHAT WE DO:

END-TO-END SECURITY TESTING ACROSS YOUR ENTIRE DEVICE ECOSYSTEM

- Hardware, firmware, network, and application testing
- Real-world attack simulations (physical and remote)
- Threat modeling and standards alignment (OWASP, NIST, ISO)
- Full penetration testing report with prioritized findings

WHAT YOU GET:

CLEAR VISIBILITY INTO RISK WITH A PATH TO REDUCE IT

- Identify critical vulnerabilities before deployment
- Reduce exposure to breaches and operational disruption
- Prioritized, business-aligned remediation plan
- Stronger security posture and compliance readiness

HOW WE DELIVER:

STRUCTURED, END-TO-END ENGAGEMENT FROM TESTING TO ACTION

- Defined testing phases across hardware and software
- Continuous collaboration with your team
- Executive-level reporting with clear next steps
- Practical guidance to fix issues and prevent recurrence

PROOF POINT:

PREVENT HIDDEN DEVICE RISKS BEFORE THEY BECOME BREACHES

A company relied on an embedded system to control a critical AC product, but it had never been fully tested for security. Leadership knew that any hidden vulnerability could expose the business to serious risk once the product was deployed.

We tested the entire system (from hardware to software) using real-world attack scenarios. The team delivered a clear report with prioritized risks, severity scores, and a practical plan to fix them.

The results revealed critical weaknesses that could have allowed attackers to take control of the system and create backdoor access. By finding these issues early, the company avoided potential breaches and moved forward with confidence, knowing where the risks were and how to fix them.

WHY SOFTSERVE

REAL DEVICE TESTING

In-house cybersecurity hardware lab to test security on physical hardware, not simulations.

PRODUCT-FOCUSED SECURITY

We secure devices before launch, not just the environments they are connected to.

END-TO-END DELIVERY

One team handles design, implementation, and testing to avoid gaps.

CRA-READY APPROACH

EU Cyber Resilience Act requirements are built into our process from the start.