SOLUTION BRIEF

Ship Demonstrably Secure Edge Devices and Stay CRA-Ready With OnLogic and Exein

Introduction

Connected edge and embedded devices are no longer a quiet corner of the network. They run production lines, fleets, medical equipment, and critical infrastructure — and they are now squarely in scope of regulations like the EU Cyber Resilience Act (CRA) and the Radio Equipment Directive (RED). At the same time, the threat model has shifted: attackers target the embedded Linux kernel, the boot chain, and post-deployment binaries, where traditional IT security tooling has no visibility.

OnLogic and Exein have partnered to close that gap. By combining OnLogic's rugged, built-to-order industrial hardware with Exein's embedded-native security stack — Analyzer for pre-deployment firmware analysis and the Photon agent for kernel-level runtime protection — OEMs and enterprises can ship devices that are demonstrably secure from silicon to userspace, and keep them that way throughout their operational life.

Let's dig in.



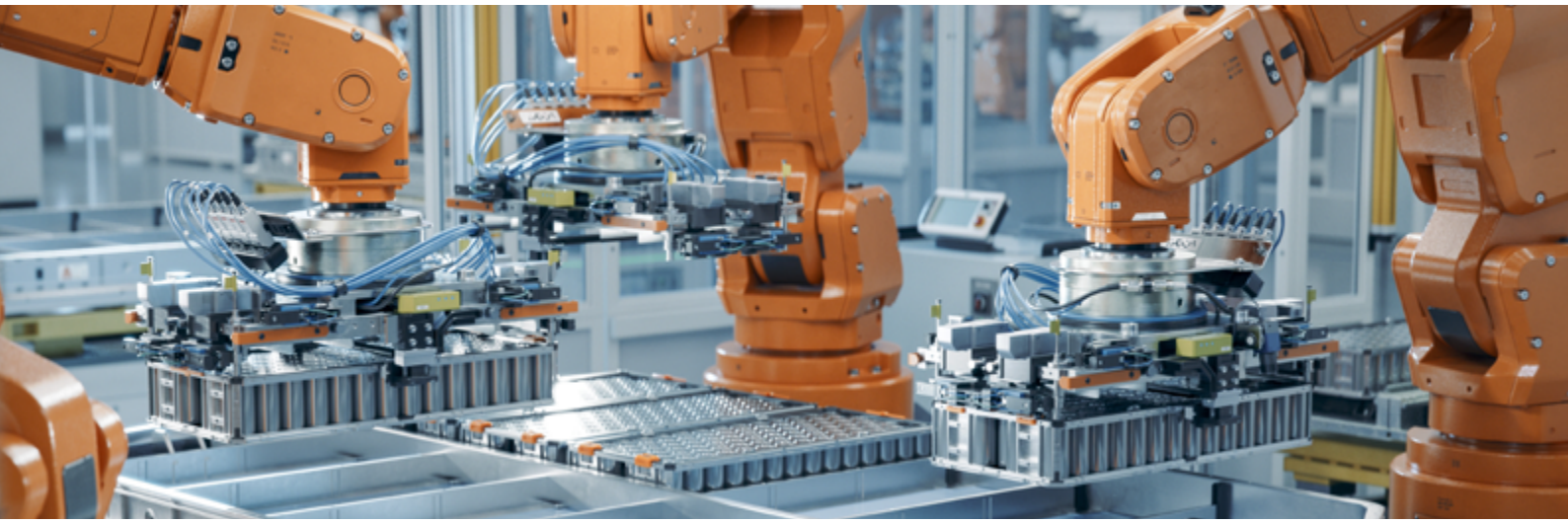
ONLOGIC × exein

The Challenge

Securing devices at the edge is fundamentally different from securing a server fleet. As OEMs and enterprises expand their embedded footprints, the same problems keep surfacing::

1. **Embedded Linux is opaque:** Production firmware is a tangle of vendor BSPs, third-party binaries, open-source components, and in-house code. Teams often cannot produce a complete SBOM, let alone confidently answer which CVEs actually apply to what is shipping.
2. **Userspace tools cannot see kernel-level attacks:** EDR and container security stacks observe syscalls and processes from above the kernel. Rootkits, LSM bypasses, and kernel-resident malware operate below that line and remain invisible.
3. **Compliance is becoming non-negotiable:** he EU CRA, RED delegated acts, and similar frameworks require demonstrable security across the product lifecycle — including vulnerability handling, secure updates, and evidence of due diligence. Documentation-only approaches will not survive an audit.
4. **Fleets are long-lived and remote:** Edge devices stay in the field for five to ten years with limited physical access. Security has to hold up across kernel updates, application changes, and a steady stream of newly disclosed CVEs — without a truck roll for every fix.
5. **Performance budgets are tight:** Heavyweight agents and signature-based scanners do not fit on industrial hardware that is already running real-time workloads, AI inference, and OT protocols.

The result: OEMs ship devices they cannot fully attest to, and operators run fleets they cannot fully see into.



The Solution: A Hardware-to-Kernel Secure Edge Stack

OnLogic and Exein deliver a turnkey, secure-by-design edge platform — rugged industrial hardware paired with embedded-native security that operates at the kernel layer.

OnLogic provides rugged, highly configurable industrial computers engineered for demanding environments. Exein delivers an embedded security platform purpose-built for Linux-based devices: Analyzer performs binary-level firmware analysis and continuous vulnerability tracking across the device lifecycle, and the Photon agent in the Runtime platform provides protection through a Linux Security Module (LSM) that enforces policy inside the kernel itself.

OnLogic systems are pre-validated for use with Exein Photon agent integrated into the OS image, anchored to the platform's hardware root of trust (Intel® Platform Trust Technology or TPM 2.0). The result is a measurable trust chain from UEFI through bootloader, kernel, and policy enforcement — and a single deployable unit that arrives ready to operate in CRA-regulated markets.

Use Cases

- CRA and RED compliance for OEMs shipping connected devices into the EU market
- Kernel-level runtime protection for industrial controllers, gateways, and edge AI appliances
- Firmware and SBOM analysis for hardware partner devices prior to mass production
- Protection of proprietary AI/ML model weights and inference pipelines at the edge
- Long-lifecycle fleet hardening for medical, energy, transportation, and critical infrastructure deployments
- Tamper detection and exploit mitigation on devices in physically untrusted environments

exein × ONLOGIC



Why Onlogic

Reliability and longevity are critical for enterprise business operations. OnLogic systems are purpose-built for industrial environments where downtime impacts throughput, safety, and revenue.

- Built-to-order systems tailored to each customer's requirements, including CPU, memory, storage, and I/O
- Industry certifications and application-specific testing for enterprise use cases
- Customization options such as custom BIOS, system images, branding, and even full custom system development
- Security features, including Intel Platform Trust Technology and optional TPM
- Long lifecycle product availability and support aligned with multi-year projects

OnLogic Features for the Edge

- Flexible I/O for direct connection to sensors, GPUs, cameras, PLCs, and other existing infrastructure
- Fanless designs for enclosed cabinets and particulate-rich edge environments
- Rugged platforms supporting wide temperature ranges and variable power input, and resistant to damage due to shock, vibration, and interference

Why Exein

Exein enables OEMs and enterprises to treat embedded Linux security as a product property — measurable, enforceable, and auditable — rather than a checklist completed at release. Exein operates where attackers actually work: inside the firmware binary before a device ships, and inside the kernel once it's deployed. Exein is the last line of defense, inside the device — operating from the kernel, where every attack ultimately has to land. Where userspace tooling stops, Exein watches the paths attackers actually use, and blocks them before they execute.

Key Capabilities

- **Preemptive kernel-level enforcement:** Exein Runtime's agent, Photon, attaches to Linux Security Module hooks to evaluate and block actions before they execute. Detection, decision, and enforcement happen in a single synchronous path in kernel space — closing the user-space roundtrip window that traditional eBPF agents leave open.
- **Lifecycle firmware analysis:** Exein Analyzer performs binary-only analysis of firmware images, producing a complete SBOM, mapping components to known CVEs, and flagging hardcoded credentials, weak cryptography, and binary hardening gaps. Continuous vulnerability tracking extends visibility well past initial release.
- **Built for CRA and RED:** Exein's controls map directly to the technical and process requirements in the EU Cyber Resilience Act and the RED cybersecurity delegated act, giving OEMs defensible evidence rather than aspirational policy documents.
- **Embedded-grade footprint:** Designed from the ground up for constrained devices, Photon runs with minimal CPU and memory overhead — small enough for industrial gateways, large enough to protect edge AI workloads.
- **Hardware root of trust integration:** Anchors the kernel-level trust chain to platform features such as Intel PTT and TPM 2.0, extending measured boot into a live, enforced runtime posture.
- **Kernel lockdown and fine-grained policy:** Restrict kernel modules, syscall surfaces, and sensitive resources with a policy model scoped to the device's intended behavior — tight enough to reduce attack surface, flexible enough to keep legitimate workloads running.
- **Fleet-wide threat intelligence:** Telemetry from deployed devices feeds back into Exein's analysis platform, so a threat detected on one device sharpens detection across the fleet.
- **Open and embedded-native:** Integrates cleanly with Yocto, Buildroot, Ubuntu Core, and other embedded build systems used across the OnLogic hardware portfolio — no replatforming required.



ONLOGIC × exein

Next Steps

Discover how OnLogic and Exein can help your organization ship provably secure edge devices, meet CRA and RED requirements with defensible evidence, and protect deployed fleets at the kernel layer where it matters most. Contact OnLogic to learn more.

North America

Call: +1 (802) 861 2300
E-mail: info@onlogic.com
www.onlogic.com

Europe

Call: +31 88 5200 700
E-mail: info.eu@onlogic.com
www.onlogic.com/eu