HARDWARIO, a leading provider of cutting-edge configurable IoT devices, has deployed S ternum on its gateways and kits. The technological partnership was announced in March 2023. Now, Hardwario’s customers can enjoy improved security on their embedded devices and enhanced monitoring.

Using S ternum for a Competitive Advantage

HARDWARIO offers gateways that enable its partners to connect sensors, PLCs, and additional devices to the internet, as well as connectivity and cloud services. Altogether, it is a comprehensive solution for enabling smart, distributed functionality through software, hardware, and services, offering solutions for manufacturing, energy, agriculture, retail, healthcare, and asset management.

HARDWARIO engaged S ternum looking to improve and augment their IoT offerings. They wanted to add security and observability capabilities that would help their partners deliver competitive, secure, and reliable IoT products and services.
The team searched for a solution that could provide the following capabilities:

- Protection from zero-day threats
- Device memory protection
- Minimal performance impact
- Easy integration with Zephyr-operated devices
- Live remote monitoring and debugging capabilities

After evaluating several options, Hardwario chose Sternum and the two companies embarked on a technology and business partnership.

HARDWARIO now offers Sternum’s security and observability capabilities to its customers as a service they can add-on.

This offering provides the company with a competitive advantage in the IoT solutions market. In the words of Pavel Hübner, CEO and co-founder at HARDWARIO: “We have long admired Sternum, for its unique ability to provide remote analysis of firmware runtime. Access to this technology improves our IoT offering and helps our partners deliver more reliable and competitive IoT products and services.”

Today, Hardwario’s customers can enjoy Sternum’s embedded security capabilities, including protection against zero-days, unknown exploits, memory attacks, info stealing, and denial of service. They can also benefit from Sternum’s observability offering, including tracking device activity and performance, AI-powered anomaly detection, and advanced investigation capabilities.
Zephyr Integration With Sternum: Easy as 123

If your device is also running on Zephyr OS, you should know that integrating Sternum with Zephyr is easy and straightforward:

1. Just add our directory and a few lines to the CMakeLists. No code changes are necessary.

2. Sternum runtime security will immediately auto-activate and can be controlled directly from the Kconfig.

3. You can deploy custom traces to set up your monitoring strategy and start collecting device-level data.

With Sternum on your Zephyr devices, you get an additional layer of runtime protection, as well as access to live and historical data, AI-powered anomaly detection, advanced investigation capabilities, and more.

Schedule A Demo To See Sternum In Action