STERNUM

Sternum secures IoT devices from within by providing real-time and on-device security solutions across technologies and industries

IoT Security – the Promise and the Threat

In recent years, IoT has been on the rise, with billions of new devices getting connected each year. The increase in connectivity is providing new functionalities and opportunities. Yet, as devices get connected, they also become unprecedently exposed to the threat of cyberattacks. Main characteristics of IoT devices, such as **low computing resources**, **excessive reliance on third-party components** and their **high diversity,** have created a real challenge for existing and traditional security solutions, leaving IoT devices more vulnerable than any other connected device. From data theft and ransomware attacks, through to harming the device itself or using it as an entry point to critical and enterprise networks, an attack on IoT devices could be destructive.

Reluctant to accept this threat, Sternum developed a multilayered solution ensuring all IoT devices are truly secured from end-to-end.

Layered IoT Security

Comprehensive IoT security is achieved through the combination of three important elements: protection, detection, and management.

Protect

To effectively secure IoT devices, attacks must be blocked in real-time and on the device itself. For this reason, Sternum developed **EIV** (Embedded Integrity Verification) and **LIV** (Linux Integrity Verification), both are proactive integrity-based attack prevention solutions, designed to protect the memory and the integrity of the device's execution flow while automatically sandboxing dangerous operations and enforcing whitelisting policies.

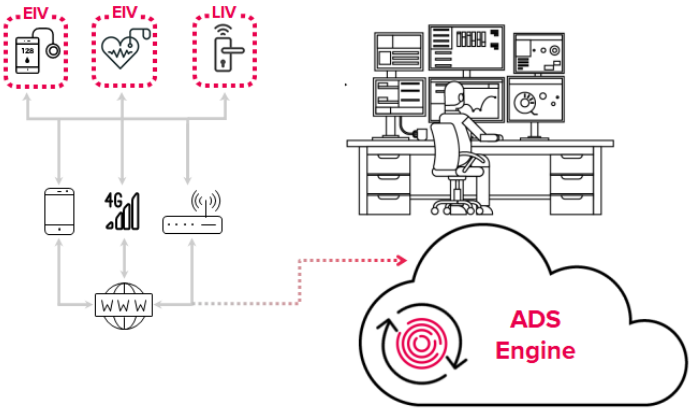
Sternum's innovative prevention approach focuses on the exploit stage of an attack in real-time. This is done by targeting the unique characteristics of an exploitation and blocking it **in real-time** when the integrity of the device is being violated. By doing so, Sternum is preventing all known, unknown and advanced attacks at the moment they strike and before any damage is done to the system. Additionally, as the exploitation stage follows finding a vulnerability in the system, Sternum's solutions are agnostic to the vulnerability being exploited, thus combating the attacks despite any vulnerability existing in the device.

Sternum's **EIV** and **LIV** are **on-device** and **software-only** solutions that protect the devices themselves. With **zero developer effort** and **no source code required**, these cutting-edge technologies are embedded automatically into the entire device's code, including closed-source code, commercial operating systems, and **third-party libraries**. Through these on-device solutions, Sternum is not only protecting the devices

THE STERNUM APPROCH

- **Deterministic:** solving security issues from the root and ensuring your devices are prepared against known and unknown threats.
- **On-device:** protecting & continuously monitoring each device (including distributed ones) from within, while not relying on any managed network connection.
- **Real-time:** preventing, detecting and alerting attacks at the exact moment of a strike, ensuring your devices are always operating while enabling immediate incident response.
- **Holistic:** all-inclusive solutions for IoT security and intelligent device analytics, that also approach the device as a whole and secures the device from end-to-end (including all 3rd party components).
- **Seamless:** seamless integration with low overhead, no additional hardware or replacing existing R&D tools. Can be applied to any IoT device (RTOS/Linux) through a platform agnostic solution.

from end-to-end, but also secures unmanaged, distributed and post-market devices (via OTA software update). Sternum's on-device solutions are also valuable for critical devices that are integral components of managed networks, and thus cannot be disconnected in case of an attack or malfunction. From medical devices that save human lives to Industry 4.0 devices that enhance our economy, Sternum ensures IoT devices are always available and secure.



Detect

Understanding that IoT security cannot be accomplished without visibility into the devices, Sternum developed **ADS** (Advanced Detection System) - a non-intrusive SDK and cloud-based analytics system offering real-time visibility into any IoT device throughout its entire lifecycle. The unique data collected from within the device, including OS and third-party components, allows advanced cybersecurity detection, threats analysis and asset management across distributed and previously unmanaged IoT devices. Cybersecurity breaches, data theft, software updates and performance events are just a few examples from the wide variety of data accessible via **ADS**.

Together with Sternum's built-in detection functions, **ADS** provides a hands-on monitoring tool that allow developers and security professionals to implement tailored monitoring traces and alerts to any RTOS, Linux or Windows OS device. With it, the benefits of **ADS** are twofold: cybersecurity detection through Sternum's core technology and tailored behavioral analytics based on your intimate access to the devices. With both data mining abilities and immediate alerts, **ADS** will help you comprehend your devices, track them and secure them before and after a security incident occurs.

For maintaining a low overhead, the security data from the devices are transmitted (and always encrypted) to Sternum's cloud via the existing connectivity functionality of the device, thus not exposing the device to new potential threats. Additionally, all the data collected by the **ADS** engine and its analysis can be accessed through Sternum's dashboard or channeled directly (via REST API) to your existing SIEM.

Manage

Sternum's tools provide real-time asset management for any IoT device, supporting risk management analysis, IoT security regulations, and production optimization. Using the intimate visibility gained by **EIV**, **LIV**, or **ADS**, Sternum empowers you with the ability to manage your devices and track their vitals, including location information, IP address, data usage, required updates, and more.

On top of real-time management, Sternum offers comprehensive IoT management tools that are OEM-oriented and set to simplify the IoT device development process. Such tools include advanced **OTA services** and **third-party risk management** (including a CBOM generator).

Combined with **ADS asset management**, Sternum's IoT management tools guarantee IoT OEMs are effectively securing their devices both pre & post-production.

ABOUT STERNUM

Sternum was founded in 2018 by a team of highly experienced research, development and business leaders. Bringing profound knowledge in embedded systems, the joint perspectives of the defender and the attacker, and an aspiration to elevate the security standard, Sternum set out to build not only uncompromising innovative technology but also to create true impact.