Sternum Embedded Integrity Verification (EIV™) and Analytics and Detection System (ADS) for Device Manufacturers

IoT devices are a dangerous vector of cyber attacks, since their software contains exploitable vulnerabilities. Patching is not an effective control and wastes resources. Other tools fail to address the root cause of the problem at scale. Vendors are responsible for the security of the devices they sell, yet most contain no on-board security, protection, or visibility.

Sternum instruments IoT devices, protecting devices from cyber risk by instantiating security and observability directly on the device, seamlessly, with negligible overhead. It prevents exploitation of known and unknown vulnerabilities in real time, nullifying them without patching. Instead of focusing on CVEs, which is an endless race, Sternum focuses on CWEs – families or types of vulnerabilities – to create autonomous, long-term protection, which is sustainable. It also provides insight on threats and the operation of the device. Sternum’s patented technology is agentless and supports all flavors of RTOS, Linux and embedded Linux, protecting the entire firmware and services and processes in the system, including third-party software and libraries.

Sternum serves as an active mitigation tool, preventing threats and instantly making devices cybersecurity without requiring an internet connection. It generates runtime alerts and furnishes data for diagnostics and continuous improvement.

Product Benefits

Painless integration via one click, zero-touch installation and management.

Harden devices in the field with real-time prevention that obviates security patches.

One security and visibility solution for all devices, including past and future generations.

Secures firmware. The United States Department of Homeland Security (DHS) has identified firmware as a single point of failure. Other products do not address this weakness.

Leapfrog complex controls and strategies that do not address root causes of breaches.

Lower exposure and effort related to patching and remediation of vulnerabilities.

Future-proof new devices and ensure continuity of protection as devices evolve.

Implement an asset management strategy with granular insights within the discovered component.

Instantaneous time-to-value and ongoing cost-avoidance.

Eliminate exposure to blackbox 3rd party and open source software, and supply chain elements.
<table>
<thead>
<tr>
<th>Embedded Integrity Verification (EIV)</th>
<th>Analysis &amp; Detection System (ADS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Description</strong></td>
<td></td>
</tr>
<tr>
<td>EIV is embedded on the device, protecting firmware and third party software from exploitation. It hooks the software, analyzes it, identifies the non-negotiable steps an attacker must take to exploit it, and expresses the steps as a unique fingerprint of exploitation. When an attack is attempted, the fingerprint triggers Sternum’s integrity verification and the attack is stopped. Sternum prevents entire families of attacks and is not exposed to new vulnerabilities or malware. It has less than 3% overhead.</td>
<td>ADS is the policy-enabling cloud platform to which prevented attacks and detected events are reported by EIV. ADS supports custom traces for extracting data for unique use cases. The dashboard allows viewing and analysis of attacks and alerts related to functional behavior. ADS’s data taxonomy supports risk and performance use cases, simplifying interpretation, guiding decision-making, and facilitating incident response, troubleshooting, continuous improvement, and quality control. Communication to ADS is one-way.</td>
</tr>
<tr>
<td><strong>Product Capabilities</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Comprehensive Protection from Memory Attacks at Runtime</strong></td>
<td><strong>Multiple Categories of Telemetry from Device Behavior</strong></td>
</tr>
<tr>
<td>It is impossible to identify and patch all vulnerabilities. Sternum’s patented Fingerprint technology blocks the pathway attackers use to exploit vulnerabilities. This protects the heap and stack, stopping entire classes of attacks such as buffer overflow, use after free, heap overflow, fileless attacks, remote code execution and more, safeguarding the integrity of memory and its components.</td>
<td>Rich data about the device is collected and transmitted to ADS, according to configurable use cases. The categories include networking, the file system, device diagnostics, connectivity, and system activity. The result is a 360 degree view of your fleet of devices and how the system is performing.</td>
</tr>
<tr>
<td><strong>Comprehensive Protection of Integrity of Execution Flow at Runtime</strong></td>
<td><strong>Runtime Alerts, Visibility &amp; Investigations</strong></td>
</tr>
<tr>
<td>Attackers attempt to divert the legitimate flow of code and use their own code or malware. Sternum stops this by ensuring the code runs only the way it was intended, stopping entire classes of attacks like return oriented programming, JOP, unallowed code execution, fileless malware, and remote code executions.</td>
<td>Sternum alerts on prevented attacks with no false positives, offering automatic remediation. Runtime alerts and extensive attack detail allow fast and focused incident response and feed any SOC / SIEM, including customers’.</td>
</tr>
</tbody>
</table>
**Embedded Integrity Verification (EIV)**

**Analysis & Detection System (ADS)**

**Product Capabilities**

**Comprehensive Protection of Command Injections at Runtime**

Command Injections are one of the most common and dangerous vulnerabilities for network devices. Eliminating all bugs during development is impossible, but preventing injections at runtime is effective and sustainable. Sternum's runtime protection verifies that all executed commands are injection-free.

**Detect Attacks on the System**

Attackers leverage logical vulnerabilities, hard coded credentials, weak OTA processes and more, to compromise devices. Sternum's system monitoring enables application security and detects attacks on logical vulnerabilities, as well as DDoS, password-stealing, log-in attempts, anomalous OTA behaviors, and connections via unauthorized ports or to unauthorized IP addresses.

**Advanced, Granular Logging for Engineering and Support**

The on-device presence and custom traces allow collection of unique, hidden data. Examples include detecting abnormal changes in computation resources, like RAM, Flash, and CPU usage; monitoring changes in usage or availability of resources to the applications or OS, like cache memory, application or reserved memory, network bandwidth; detecting unexpected delays or impaired response time of some functions or tasks; checking if services or application containers are not running.

**Product Characteristics**

Breadth and depth of coverage: Eliminates entire families of attacks (CWEs). Prevention and detection of the most dangerous threats in the MITRE top 25, including memory, command injections, and system-level attacks. Applies control flow integrity in real-time to prevent malicious code execution. Includes all processes and services. Unmatched performance in RIPE testing. Includes all firmware.

Protects manufacturers' firmware, suppliers' devices, 3rd party and open source software, and connectivity components.

Proactive mitigation, with no dependencies on updates, signatures, or any externalities.

Negligible overhead (< 3%) and no performance impact. No changes to code, platform, or logic.

Runtime alerts, data and analytics enable delivery of security as a service.
Setting Up Sternum

Sternum protects any device with a one-click operation. Remote installation is supported. Source code is not required.

**Step 1**
- Define Use Cases and Policies
- Install EIV
  - Direct – Remote *
  - CI/CD
  - IDE
- Configure ADS
  *Linux only

**Step 2**
- Deterministic Protection Achieved
- Consume and Use Alerts and Reports
- Compliance Achieved

---

**Value for Device Manufacturers**

**Security**
- Deploy on new and legacy devices
- Avoidance of patching – active mitigation - hard ROI
- Customer confidence

**Observability**
- Troubleshoot issues
- Operationalize insights
- Data insights from device fleets

**Compliance and Regulatory**
- FDA
- NIST
- UL 2090
- IEC 62443
- EN 303 645

**Services Revenue**
- Security and alert services for customers

---

[Sternumiot.com](https://sternumiot.com) | Working with: Medtronic | NXP | arm

---

04
Summary

Vulnerabilities are inevitable, numerous, and different. They should be assumed in all firmware and on every device. The number is growing as the volume of code increases. Chasing and mitigating them reactively is unproductive. Sternum is a proactive, deterministic, runtime protection that neutralizes entire families of attacks at runtime. It is easy to install, lowers the risk of breach, and safeguards the reliability of embedded device ecosystems.

Email: sales@sternumiot.com to book a demo.