A joint advisory from the US Cybersecurity and Infrastructure Security Agency (CISA) and FBI underscored the heightened threat of ransomware attacks against healthcare providers. Medical device manufacturers (MDMs) now face significant cybersecurity challenges. Recent requirements by the EU’s Medical Device Regulation (MDR), the US FDA, and the US 2023 Consolidated Appropriations Act (Omnibus) Bill evidence a constantly changing regulatory landscape.

MDMs must now meet rigorous security measures during product design, development, and testing phases. Post-market surveillance must include data collection and analysis of adverse events. Such compliance requires a significant investment in resources and expertise to address complex technological and operational challenges. Failure to do so could result in potential harm to patients, in addition to legal and reputational risks.

Such regulatory compliance challenges include:

- **Device resource constraints** – MDMs are unable to meet the intent behind requirements for vulnerability management and post-market surveillance with runtime solutions adapted from IT security because they compromise device performance. This leaves dangerous security gaps.

- **Increased number of zero-day vulnerabilities** in third-party libraries used extensively in device development

- **Rapid evolution of cyber attacks** – As bad actors become more sophisticated and creative at leveraging new attack vectors and methods (and evolving technology presents them with new possibilities), MDMs need to continuously ensure devices are protected from the latest generations of threats

- **Growing post-market surveillance requirements for compliance**, along with minimal visibility into deployed devices (with no way to collect, store, and extract live data)

- **Tight incident reporting deadlines require expedient**, granular data collection and processing
Sternum helps MDMs meet regulatory requirements

Working with the world’s largest medical device manufacturers, Sternum has a proven track record of meeting and exceeding regulatory expectations. It offers an easy, cost-effective way to achieve compliance (FDA, MDR, NIST, et al.) for both legacy devices as well as new products.

Armed with Sternum’s runtime security and monitoring capabilities, MDMs are able to:

- Meet new requirements with minimal investment and remain prepared for additional ones
- Integrate runtime protection into security by design to protect against future cybersecurity risks
- Strengthen post-market surveillance capabilities

How Sternum addresses relevant MDM regulatory concepts

To ensure you meet the full range of regulatory requirements, Sternum supports the following guidelines and regulations:

- FDA 2022 Guidance: Cybersecurity in Medical Devices
- 2023 US Omnibus Appropriations Bill
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- MDCG 2019-16 Guidance on Cybersecurity for medical devices (MDR)
- The NIS2 Directive
The table below shows what they mean for MDMs’ products and processes, and how Sternum helps.

<table>
<thead>
<tr>
<th>Regulatory Requirement</th>
<th>What it Means</th>
<th>How Sternum Helps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices need to be “secure by design”</td>
<td>What it Starting March 2023 – Current cybersecurity processes will not be enough for the FDA as a result of the Omnibus Bill. The bill provides authority for the FDA to implement regulatory guidelines, such as implementing the “secure by design” model. Legacy devices already in the field can be affected as well. “Secure by design” means security is built into products and developments processes, for example: - Software requirements - Risk assessment - Security controls - Secure product development framework (SPDF) and more. Security should not be viewed as an add-on at the end of the design phase.</td>
<td>Sternum’s platform is seamlessly integrated into both new and legacy devices—the entire fleet is covered. Sternum’s platform is embedded within MDMs’ software. It provides proactive, agentless, runtime security from day one, with continuous detection and mitigation of zero-day attacks throughout the entire product lifecycle—from development to production. Sternum alerts regarding suspicious device and user behaviors in addition to security issues Staying ahead of future security risks, Sternum enables MDMs to gain the trust of regulators and customers, and accelerate time-to-market by demonstrating advanced detection and mitigation capabilities. MDMs using Sternum’s proactive protection stay ahead of new security threats and new regulatory requirements.</td>
</tr>
<tr>
<td>Regulatory Requirement</td>
<td>What it Means</td>
<td>How Sternum Helps</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Implement vulnerability management process</td>
<td>Manufacturers are now required to implement a plan to continuously identify, mitigate, and communicate vulnerabilities throughout the product lifecycle. Regulators no longer expect a vulnerability-free device, but rather a focus on prevention of exploitable vulnerabilities. Specifically, many vulnerabilities stem from use of third-party libraries (supply chain security) that are hard to monitor and mitigate. Growing reporting requirements also put MDMs under the spotlight to share information with hospitals “in a timely manner” when new vulnerabilities arise.</td>
<td>On top of continuous device protection throughout the device lifecycle, patented Sternum fingerprinting technology identifies exploitable vulnerabilities. It detects and mitigates vulnerabilities that matter the most, reducing time and effort of patching. Assure regulators with confidence that devices are secure. Sternum agentless security enables protection from third-party software and supply chain risks. With Sternum automatic security alerts and granular data collection, MDMs can easily and quickly get notified, investigate, extract data, and generate relevant reports.</td>
</tr>
<tr>
<td>Verification and validation of security controls</td>
<td>Like all product and software requirements, security requirements and controls must be tested during V&amp;V. New regulatory guidelines highlight this need even more. MDMs are to provide security testing reports as part of regulatory submissions. In addition to the usual risk assessment, MDMs must demonstrate they have proper controls and mitigations in place and prove they work as expected.</td>
<td>Sternum’s coverage provides regulators with evidence of threat mitigation, e.g., detection of and protection from exploits of zero-day vulnerabilities, thereby demonstrating effective risk control measures.</td>
</tr>
<tr>
<td>Regulatory Requirement</td>
<td>What it Means</td>
<td>How Sternum Helps</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Expanded post-market surveillance requirements</td>
<td>New guidelines exist for monitoring and handling emerging security risks for products already on the market, even though post-market surveillance is not new. Identifying risks and vulnerabilities at the design and development stage no longer satisfies regulators. MDMs are required to identify and respond to new security risks as they emerge in the field. Outside security, manufacturers still need to continuously collect external device data for product assessment and device use to complete annual reports for regulatory bodies.</td>
<td>With Sternum’s automatic alerts, MDMs get notified on emerging security issues, can investigate and report incidents, and monitor security posture for in-field devices. Sternum collects live and historical device-level data, providing a continuous view of the device’s condition and integrity, as well as its performance, and security posture. MDMs can collect and monitor integral device information on their entire fleet for risk assessment, performance improvement, and more. MDMs get access to all the data needed for post-market surveillance reports.</td>
</tr>
<tr>
<td>Expanded incident reporting requirements</td>
<td>New regulatory requirements mandate strict timelines for device incident reporting, especially in relation to security. In some cases, it’s as little as 24 hours from becoming aware of an incident. MDMs are now required to produce detailed incident reports—including device information, root cause analysis, mitigation plan, and more within a very short time frame.</td>
<td>Sternum automatically alerts about security issues and collects all relevant data to investigate and report incidents. This permits extraction and processing of granular data for detailed reports in a very short amount of time. MDMs can customize device traces and alerts to instantly receive data warning of a safety incident or device malfunction in advance of complaints and to diagnose them.</td>
</tr>
<tr>
<td>Regulatory Requirement</td>
<td>What it Means</td>
<td>How Sternum Helps</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Expanded incident reporting requirements</td>
<td>Incident reports should now include information about how the entire device fleet could be affected. Routine investigation and reporting, such as customer complaints and CAPAs, require more detailed device information. MDMs have a growing responsibility to provide hospitals with integral device information and event updates for incident response.</td>
<td>Sternum’s event tracing supports MDMs in investigating security events, CAPAs, and customer complaints by quickly identifying the root cause. For each event, Sternum enables downloading a report with all event details—including a timeline of events leading up to an issue, device details, etc. MDMs can immediately advise health delivery organizations (HDOs) about an event, thus permitting swift resolution and remediation.</td>
</tr>
</tbody>
</table>

**Sternum is easy to integrate and works with existing platforms and OS**

Sternum is already deployed on millions of connected medical devices. Its proactive, embedded platform aligns with the tooling and process strategies of MDMs, as well as with their performance and resource constraints—with:

- On-device, one-time integration for any RTOS and Linux OS
- Near-zero overhead (< 3%)
- No disruption of the code
- Deep experience and know-how of connected medical devices
- No need for new FDA submission
By using Sternum, MDMs can:

**Make compliance part of the device lifecycle and streamline compliance processes**
From design and development to production, Sternum enables proactive protection and monitoring for the most recent (and future) cybersecurity regulations and post-market surveillance requirements. It enables quality assurance, compliance, and product teams to optimize compliance processes and gain regulators’ trust.

**Ensure patient protection from cyber threats**
Sternum provides MDMs with peace of mind. Proactive, runtime self-protection and advanced threat detection and response ensure that patients are protected from cyber-attacks.

**Accelerate time-to-market**
Shorten device design and development by optimizing compliance processes. Penetrate new markets quickly and easily by meeting changing regulatory requirements and increasing regulatory resilience.

**Gain competitive differentiation**
By offering products with proactive protection from exploitation of vulnerabilities and continuous monitoring, MDMs offer more value to their customers – HDOs, individual medical practitioners, and home-care patients – giving them data and assurances that support their compliance requirements.

**Extend device life**
By adapting devices to new regulations and avoid obsolescence.

Learn how Sternum helps meet regulatory requirements

Request a demo →