
Eliminating FDA 524B
"Refuse to Accept" Obstacles
Ensure On-Time Medical Device Product Launches
FINITE STATE

50% of the connected medical devices harbor critical cybersecurity risks, and 75% of infusion pumps have at least one critical vulnerability that could threaten patient safety if exploited. **The proliferation of connected medical devices hasn't taken place in a vacuum. Globally, some 25.4 billion connected devices are expected to be in use by the end of this decade, and the costs resulting from breaches of their systems are expected to reach $20 billion.***

Attackers love the threatscape cultivated by the explosive growth of IoT technology. The ever-increasing complexity of software supply chains generates new and dangerous opportunities for CVEs and configuration errors to ship in finished connected medical devices, and the proliferation of remote access to IoT devices has fueled new vectors through which attackers have pursued their exploits.

To date, connected medical device security hasn't kept pace. Most AppSec tools do not work on embedded and connected medical devices. Limited visibility into software supply chains has rendered risk management opaque and ineffective, as evidenced by the low priorities these risks have received from manufacturers and the infrequent patching cycles to reduce these risks.

The US Food and Drug Administration (FDA) has taken notice with a strong stance on the importance of cybersecurity in medical devices, given the nature of these emerging threats and the impact on patient care when cybersecurity is compromised.

*https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities

The FDA's "Refuse to Accept" Policy and Section 524B

Section 3305 of the Omnibus bill features section 524B, which prioritizes the cybersecurity of medical devices as the agency moves from its historical stance of recommended guidance to a 'Refuse to Accept' stance on the premarket submissions it receives. Section 524B, entitled "Ensuring Cybersecurity of Medical Devices," grants the agency statutory authority to accept or refuse submissions based on whether applicants meet new cybersecurity standards.

The agency's new "refuse to accept" authority under section 524B takes enforcement to a new level, and can potentially delay or halt the pre-market review process, if manufacturers fail to comply with the cybersecurity requirements outlined in the FDA's guidance.

This guidance targets insufficient documentation of risk assessments, lack of vulnerability assessments, and inadequate strategies for risk mitigation as primary reasons why a premarket submission may not advance. To avoid delays in product approvals and ensure a smooth regulatory process, medical device manufacturers must now prioritize compliance with section 524B requirements.

How Finite State Can Help

The Finite State Next Generation Platform plays a vital role in assisting medical device manufacturers in meeting the FDA's expectations for medical device cybersecurity. By leveraging our solution, manufacturers can proactively address the key elements outlined in the FDA section 524B guidance, thereby enhancing their chances of acceptance and accelerating the approval process.

With Finite State's Next Generation Platform, medical device manufacturers can establish a robust software supply chain security program, meet the FDA's expectations, and deliver safe and secure devices to the market while gaining the software transparency they need to minimize delays in the regulatory review process.

Finite State's Next Generation Platform encompasses comprehensive vulnerability assessments, threat intelligence, risk management, compliance reporting, and continuous monitoring capabilities, all tailored to provide the continuous visibility manufacturers need to build software supply chain security and meet the FDA's stringent cybersecurity requirements. By using our platform, manufacturers can demonstrate their commitment to patient safety, data protection, and regulatory compliance, mitigate the risk of FDA refusal, and streamline their path to market.

The Federal Food, Drug, and Cosmetic Act (FD&C Act) Section 524B(a) indicated that the sponsor of a premarket submission for a cyber device needs to include data that the cyber device meets the cybersecurity requirements in section 524B(b) of the FD&C Act. The following table maps Finite State capabilities to the 524B cybersecurity requirements:

FD&C Act Section 524B(b) Requirements	Finite State Next Gen Platform Capability
Submit a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures	The Finite State Next Gen Platform helps medical device manufacturers meet FDA requirements for comprehensive vulnerability assessments. Our firmware binary analysis and vulnerability correlation features utilize advanced scanning techniques to identify common security flaws, configuration errors, and software vulnerabilities. Our platform provides access to updated threat intelligence feeds, including known vulnerabilities and emerging cyber threats specific to medical devices. By correlating risk data across more than 120 scanning tools, the platform enables proactive identification of potential risks and a prompt response to emerging threats.
Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems	The Next Gen Platform facilitates risk management through our rigorously defined risk scores and remediation guidance. The platform assesses the potential impact of identified vulnerabilities on patient safety, data integrity, and overall system security. Risks are prioritized based on severity, exploitability, and other relevant factors, providing guidance on risk mitigation strategies and best practices to reduce the overall risk profile of the medical devices.
Provide a software bill of materials, including commercial, open-source, and off-the-shelf software components	The Finite State Next Gen Platform is integral in evaluating the security posture of third-party vendors supplying components or software used in medical devices. With our end-to-end Software Bill of Materials (SBOM) generation and management, the Next Gen Platform assesses vendor cybersecurity practices and enables reviews of their compliance with relevant regulations. Our platform provides guidance on selecting and managing vendors to mitigate software supply chain risks.

Why Choose Finite State

End-to-End SBOM Solution

- The only solution in the industry to successfully demonstrate SBOM generation, ingestion and dynamic management across multiple firmware image formats in the first-ever S4x23 SBOM Challenge

Best-in-Class Binary Software Composition Analysis

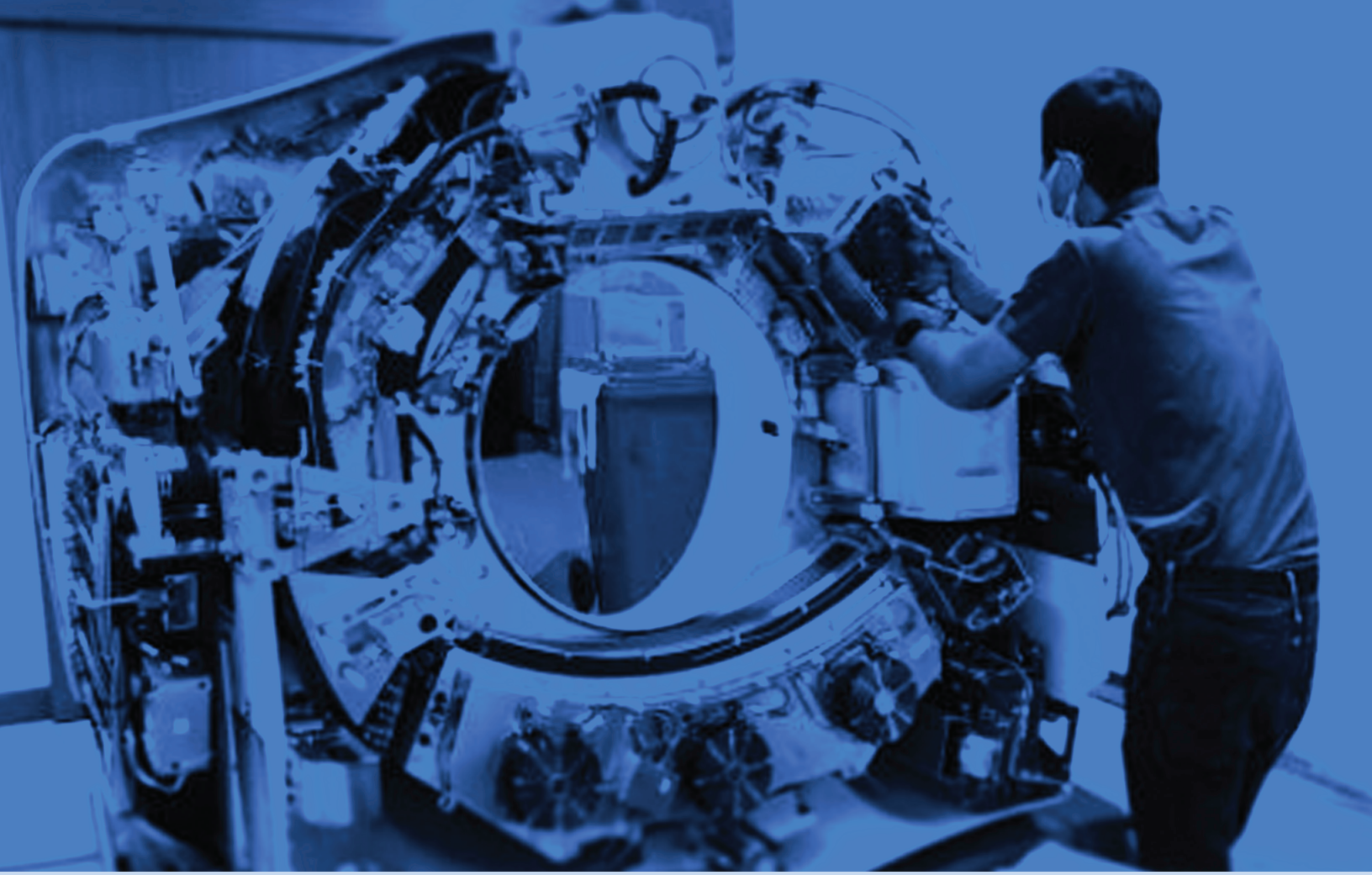
- Revealed 5X the validated vulnerabilities compared to others in the industry at the first-ever S4x23 SBOM Challenge
- Wide breadth of coverage for file formats, operating systems, instruction sets, and platforms
- Unsurpassed depth of analysis with deep binary feature extraction and matching

Best-in-Class Software and Supply Chain Risk Management

- Ingested 6X the vulnerability and threat intelligence sources compared to others in the industry during the first-ever S4x23 SBOM Challenge by integrating 120+ tools for a unified view of software supply chain risk, correlating AppSec findings and managing vulnerabilities
- Provides an intuitive score that empowers teams to prioritize and act on vulnerabilities quickly, building resilience and stewardship into their security operations

Domain Expertise

- Leading software supply chain security and risk company with a collective of security experts
- Extensive experience in medical device cybersecurity and compliance with regulatory standards
- Our team comprises experts with deep knowledge of medical device security, FDA regulations, and industry best practices



Conclusion

For medical device manufacturers seeking to comply with FDA 524B, the Finite State Next Generation platform eliminates the “Refuse to Accept” roadblock. The platform allows products to be shipped on time with a validation of their security, ultimately shortening time-to-market.

Finite State automation capabilities help scale your product security program and identify risks in code, even if it’s not your own. The platform’s advanced threat intelligence enables you to take charge of your threat landscape. In addition, Finite State’s best-in-class binary SCA ensures a more complete SBOM. With zero installation required, you can go from zero to SBOM in just a few hours, making the deployment process frictionless.

About Finite State

Finite State enables the teams responsible for the most critical connected infrastructures to protect the devices we rely on every day through market-leading software threat, vulnerability, and risk management.

By analyzing every piece of information in device firmware, from third-party code to configuration settings, Finite State enables secure device manufacturing at scale. Our products and services integrate seamlessly into existing development and SecOps processes and provide actionable security metrics to address product and supply chain risk.

FINITE STATE

finitestate.io