USE CASE

Medical Devices: FDA and EU MDR/IVD Compliance

INDUSTRY
Medical Device

OVERVIEW

In response to attacks on medical devices, regulators around the globe are implementing cybersecurity requirements that push manufacturers to develop devices that are resilient and able to protect patient safety and privacy. The FDA in the United States and European Union requirements, like theMedical Devices Regulation (MDR) and In Vitro Diagnostic Medical Devices Regulation (IVDR), focus on a lifecycle approach to medical device software development, with requirements from design through to postmarket. RunSafe Security provides medical device manufacturers cybersecurity solutions to maintain compliance with FDA and EU requirements while reducing the risks associated with delayed patching and supply chain vulnerabilities.

CHALLENGE

The FDA now requires that manufacturers provide a Software Bill of Materials (SBOM) that lists all commercial, open-source, and off-the-shelf software components. For medical devices, especially legacy ones and those written in C/C++, generating SBOMs is a challenge.

Additionally, in the U.S. and the EU, regulators are focusing on a total lifecycle approach to device security, requiring risk management and security measures from product design to post-market monitoring. Vulnerability identification and patching devices post-market is particularly challenging, demanding significant developer time and resources.

SOLUTION

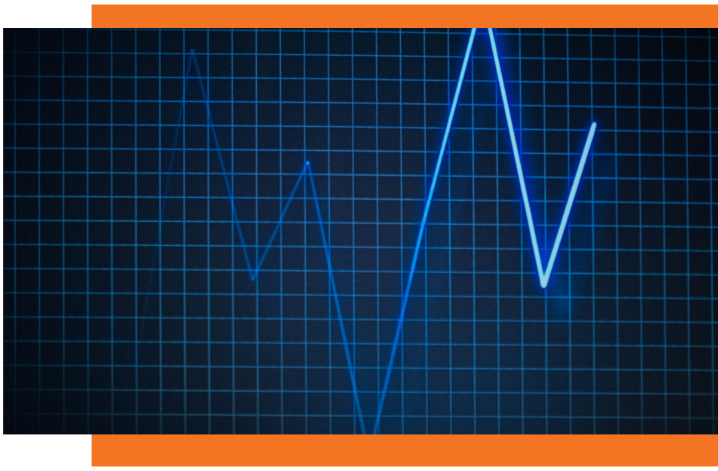
RunSafe helps medical device manufacturers achieve FDA approval and EU compliance by integrating automated vulnerability mitigation and code protection measures, enabling compliance with Secure by Design requirements and accelerating a secure go to market process.

Key features of RunSafe's solution include:

- **Build-time Software Bill of Materials:** RunSafe's build-time SBOMs for C/C++ generate a complete list of all applications, libraries, and files used during a chosen build, including information about the source material, target, and dependencies.
- **Automated vulnerability identification:** RunSafe's technology identifies vulnerabilities present in software and quantifies available risk reductions, allowing medical device manufacturers to prioritize mitigations and move forward with software releases.
- **Continuous protection for legacy and new medical devices:** RunSafe applies Load-time Function Randomization to proactively safeguard medical devices throughout the device lifecycle from the entire class of memory safety vulnerabilities—even before patches are available. This allows manufacturers to streamline the patching and update process, knowing that even if vulnerabilities are found, they are safe from exploitation with RunSafe Protect deployed.

KEY FEATURES

- Complete Software Bill of Materials
- Pre-market submissions / post-market management
- Automated mitigation and code protection



Examples

Automated mitigation and risk reduction: A medical device company was seeking a way to accelerate its time to FDA approval by dramatically reducing its attack surface and minimizing the severity of vulnerabilities so it can optimize its scanning, fixing, and patching processes. With RunSafe, its devices are protected from exploitation for both known and unknown vulnerabilities.

Addressing software supply chain risk: One product security team leveraged RunSafe's Software Security Platform for embedded developers to extend its return on investment by rolling out a centralized way to generate SBOMs, identify vulnerabilities, and integrate vulnerability mitigation within its build tools.

RUNSAFE
SECURITY

🖥 RunSafeSecurity.com
☎ 571.441.5076
✉ Sales@RunSafeSecurity.com

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals.