

HEIMDALL SBOM & VULNERABILITY MANAGEMENT




Heimdall's vulnerability management tool enables automatic generation of a Software Bill of Materials (SBOM), identifies known & exploitable vulnerabilities, and enables prioritized risk reduction in an easy, economical, and reliable way

SHIFTS IMPACTING MEDICAL DEVICE MANUFACTURERS (MDMs)

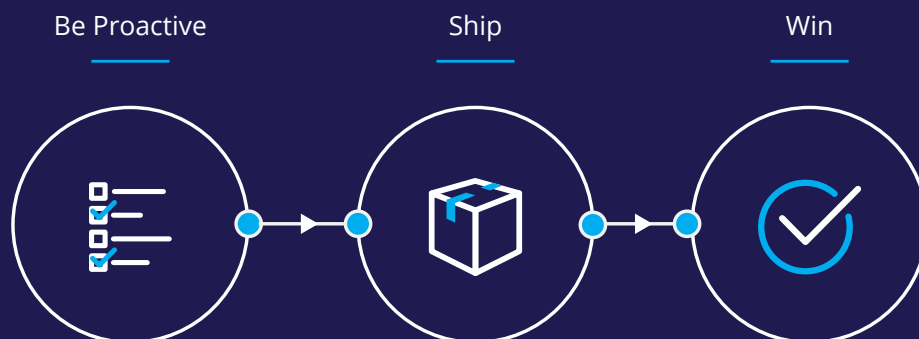
MDMs used to be able to ship a device, hope there were no cybersecurity issues, and address problems as they were found. Today, by utilizing MedCrypt's healthcare-specific tools and APIs, leading MDM's can more easily, efficiently, and proactively build security features into their devices and gain visibility into new and legacy devices to meet regulatory and customer security requirements.

SCENARIOS - WHAT DO YOU DO TODAY?

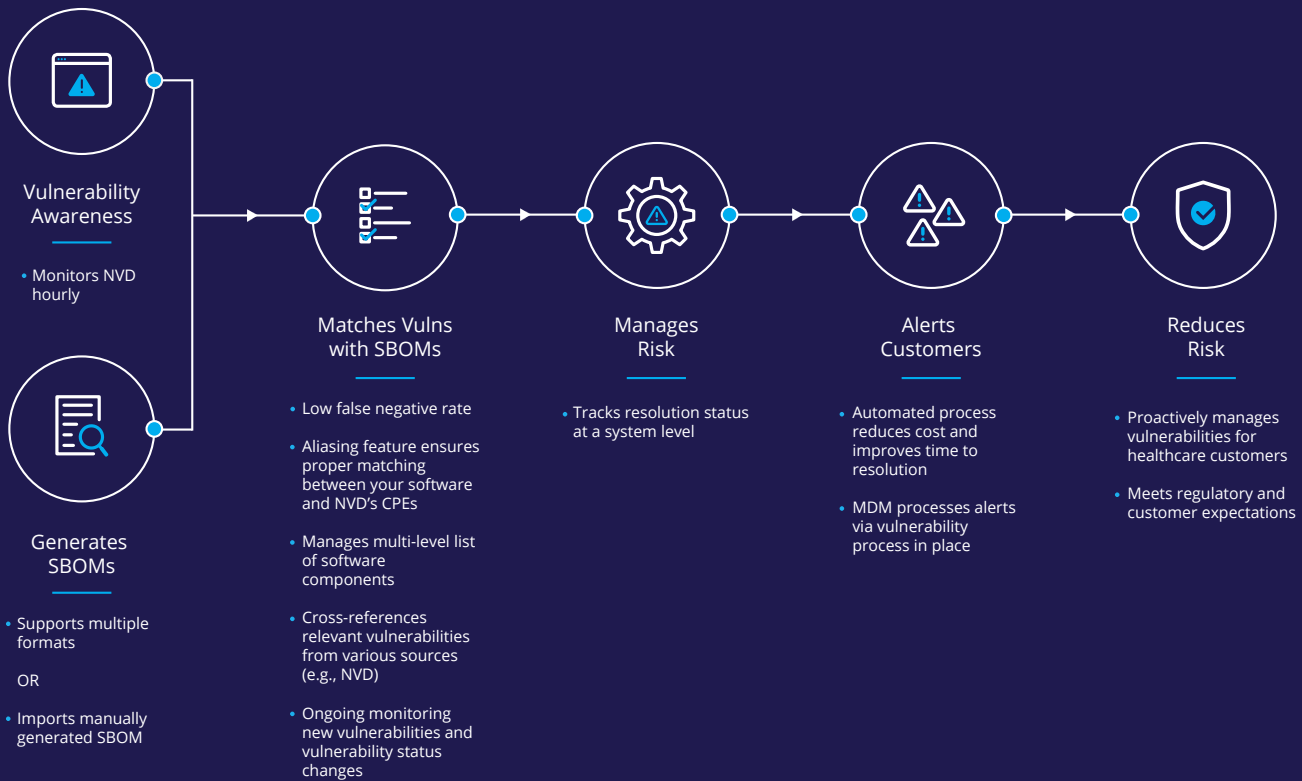
If another WannaCry-like attack began to actively exploit a Windows vulnerability, is your current SBOM strategy up to the task?

- 
 Could you rapidly identify which of your products and their respective versions are impacted? Or, will it be all hands on deck to search through spreadsheets or re-scan every software build to see if they are affected?
- 
 Could you swiftly determine the severity of the vulnerability? Or, will you need to manually assess each affected device?
- 
 Will you be able to proactively help your customers know which devices are at risk? Or, will your team be scrambling through databases to determine which affected device versions are deployed at which hospitals, while you search for the CISO contact to deliver the bad news?

WITH HEIMDALL YOU COULD:



HOW HEIMDALL WORKS



WHAT HEIMDALL BRINGS TO YOUR SBOM-BASED VULNERABILITY MANAGEMENT

Building a vulnerability management system and processes that consider the device SBOM is an essential prerequisite for security best practices. Such an approach serves a number of critical purposes:

- Generate SBOMs in consistent manner across product lines and versions
- Full visibility of all components of the device software (including their dependencies)
- Seamless integration into existing vulnerability management process
- Support hospital requests for SBOM and vulnerability data to support risk management and incident response
- Forensically link vulnerabilities to device event behavior
- Address regulatory requirements for premarket security risk management and postmarket surveillance and maintenance - for new and legacy devices

ABOUT MEDCRYPT

MedCrypt provides proactive security for healthcare technology. MedCrypt's platform brings core cybersecurity features to medical devices with just a few lines of code, ensuring devices are secure by design. MedCrypt announced a \$5.3 million Series A funding round in May of 2019, bringing the total funds raised to \$8.4 million with participation from Eniac Ventures, Section 32, Y Combinator, and more. The company is based in San Diego, California. For more, please visit www.medcrypt.com.

San Diego, California, USA

(877) MDC-RYPT (877-632-7978)

info@medcrypt.com | www.medcrypt.com