# CANARY - MONITOR DEVICES IN THE FIELD

Canary is a remote monitoring agent that detects security events in deployed devices, filters out false positives, and informs mitigation strategies. Gain visibility into devices with limited engineering effort.

## SHIFTS IMPACTING MEDICAL DEVICE MANUFACTURERS (MDMs)

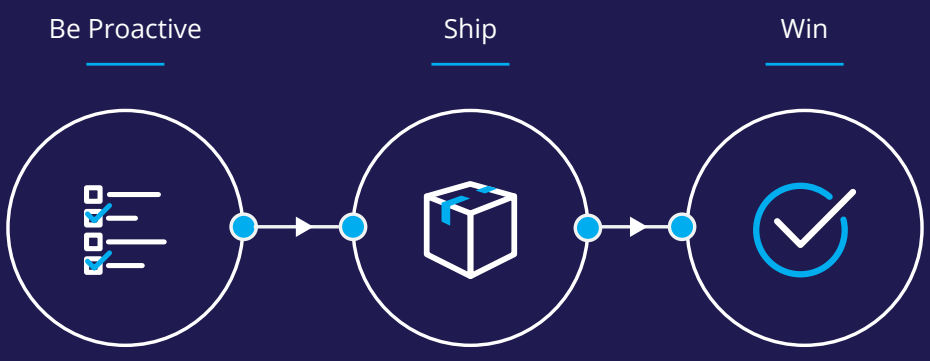
MDMs used to be able to ship a device, hope there were no cybersecurity issues, and address problems as they were found. Today, by utilizing MedCrypt's healthcare-specific tools and APIs, leading MDM's can more easily, efficiently, and proactively build security features into their devices and gain visibility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

## SCENARIOS - WHAT DO YOU DO TODAY?

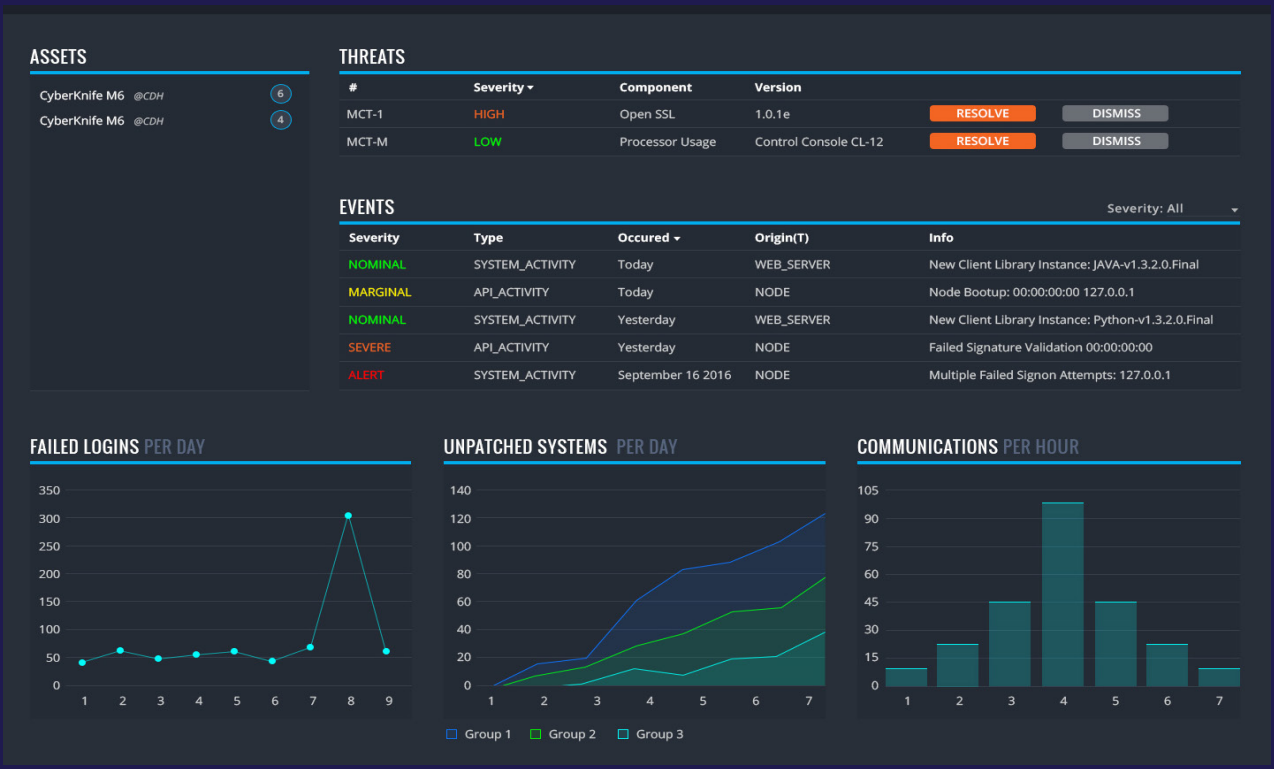
As connectivity proliferates across medical devices, postmarket monitoring is critical to ensure continued clinical operation, troubleshooting device issues, and identification of potential cybersecurity events to be investigated.

- Could you rapidly identify the version of software running on a device in an inconsistently connected environment? Or, will it be a guessing game to try and understand a device version when a hospital calls to report an entire fleet is acting annomolously?
- Could you proactively determine if a device has been compromised and is acting suspiciously? Or, is there an absence of forensic-grade evidence obtained, tracked and reviewed?
- When the device user calls to raise an issue about a device, do you already have event data and device metadata available to begin troubleshooting? Or, will your team have to deploy a technician to obtain device data, , while you search through service level agreements to ensure you aren't in bigger trouble?

## WITH CANARY YOU COULD:



## HOW CANARY WORKS




## WHAT CANARY BRINGS TO YOUR POSTMARKET MANAGEMENT

Building a device that is proactively secure is just the beginning. As stated in the 2016 FDA Postmarket Management of Cybersecurity in Medical Devices, managing cybersecurity throughout the product lifecycle is critical to ensure patient safety. Canary enables security best practices through an easy to install agent and a cloud-based service with limited engineering effort. With Canary you can:

- Detect security events, such as unauthorized communications (ex. network, application or external device), or commands from non-trusted sources (ex. man-in-the-middle attack).
- Gain visibility into version of applications running on a device, specific to a serial number of device.
- Integrate security features across the entire MedCrypt platform.
- Support hospital requests for vulnerability data to support risk management and incident response.
- Forensically link vulnerabilities to device event behavior.
- Address regulatory requirements for 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 $9.4 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.

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

medcrypt