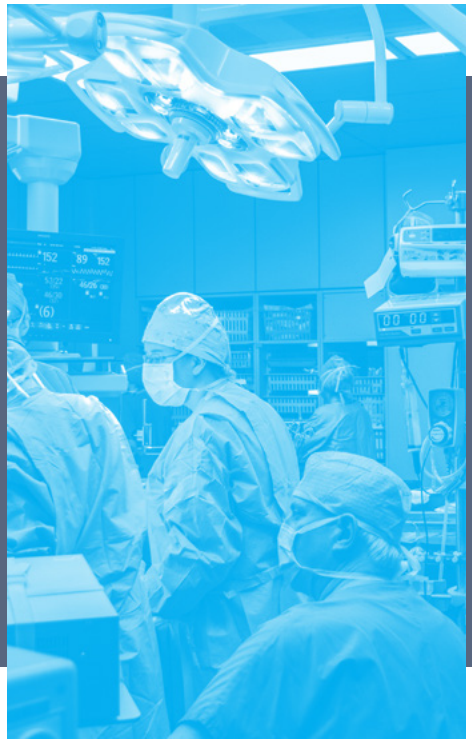
IMPACT OF MONITORING ON MEDICAL DEVICE VULNERABILITIES

Background:
In prior white papers we addressed the increasing concern about cybersecurity in devices and the range of technologies that can be helpful in addressing this concern. In the following pages we will highlight the impact behavior monitoring and intrusion detection can have on the security posture of medical devices.

READERS WILL LEARN

Cybersecurity concerns arise across procurement, engineering, R&D, quality and legal departments in an organization. This whitepaper will inform decisions around monitoring strategies in your organization:

- Common Vulnerability Scoring System (CVSS) ratings for 41.7% of vulnerability disclosures could be lowered through the implementation of monitoring solutions.
- Vulnerabilities that would otherwise be 'uncontrolled' and potentially require a recall, could be considered 'controlled.'
- Trend in medical care delivery outside of healthcare delivery organizations (HDOs) requires a device based monitoring solution that does not depend on HDO management.



SECTION I: STATE OF THE INDUSTRY

VULNERABILITY STATISTICS

U.S. HDOs now exceed 900,000 beds, with an average of 10 - 15 devices per bed, that amounts to more than nine million devices. As devices increase in quantity there has been a related increase in vulnerabilities disclosed by medical device vendors.The ICS-CERT Advisory Database was analyzed to find all advisories related to connected medical devices. The data extracted from these advisories can be found here. In total, 63 advisories were released between 2013 and March 31, 2019, consisting of 146 total vulnerabilities.

Advisories were divided into two time frames—before and after the FDA Postmarket Management of Cybersecurity in Medical Device Guidance (which was finalized on December 28, 2016). Among the data points examined is the Common Vulnerability Scoring System (CVSS) score assigned to vulnerabilities within an advisory.

Time Frame	Oct 23, 2013 - Dec 28, 2016	Dec 29, 2016 - March 31, 2019
Number of Advisories	12	51
Total vulnerabilities disclosed in advisories	37	109
Average vulnerabilities per month	0.95	4.19
Companies	6	24
Mean vulnerabilities CVSS scores[1]	7.30	6.87

[1] CVSS transitioned from version 2.0 to version 3.0 during the period from October 2013 to December 28, 2016, the negligible impact of which has been assessed as part of Whitepaper 1.

REGULATORY REQUIREMENTS

The October 2018 FDA premarket cybersecurity guidance requires medical device manufacturers (MDM) design devices with security in mind. This guidance will be the measure for 510(k) clearance for new medical devices, and outline industry leading practices for 'live' devices. While guidance details are being finalized, there are five themes MDMs must consider in their product security strategy: risk-based strategy, security development lifecycle, cryptography, postmarket maintenance, and device behavior monitoring.

In this whitepaper, we examine the potential impact of monitoring on vulnerability disclosures to date.

WHAT IS MONITORING?

The objective of monitoring is to determine if a device is acting abnormal to an established baseline of behavior and then determining whether that is attributed to a vulnerability being exploited or another potential cause. To monitor a device, the footprint a device leaves is tracked to determine a baseline of operation in normal circumstances. Some of the attributes to be monitored include:

- Bandwidth usage, internal CPU and memory usage, number of connections
- Free disk space, log entries, running processes and services, application behavior
- Configuration file integrity
- Application specific functions, like API events
- User authentication attempts

As a clarification, device monitoring activity does not mean reviewing patient outcomes, nor does it involve access to personal health information. It encompasses device diagnostics that inform understanding if a device is operating as intended.

Two main mechanisms for medical device monitoring are:

1. HDO network monitoring
2. Capability built into a medical device

The most robust security posture includes a combination of both HDO and medical device based monitoring. **Current regulatory guidance further clarifies that HDO monitoring does not diminish the need for device based monitoring.**

HDO network monitoring is often done with the intention of ensuring availability of patient data. It is critical to have access to patient data when clinicians need it, and to be sure multiple IT systems work together to deliver clinical care. These systems include imaging devices, imaging data, information systems and a central communication server. However, not all devices come with software that allows the hospital IT (HIT) team to track device activity. This can mean HIT will have little knowledge on how to manage the devices and ensure they are operational.

As required in the October 2018 FDA premarket cybersecurity guidance, MDMs must delivery medical devices with the ability to alert on abnormal cybersecurity behavior. Device-based monitoring is useful in the clinical and 'at home' environments. Devices designed to operate outside the hospital, like remote monitoring devices sent home with patients, are increasing in number and require additional consideration, as hospitals cannot assess the 'at home' cybersecurity environment of patients. Instead, the HIT team relies on monitoring capabilities built into devices, while leaning on MDMs for 'at home' issues patients experience with their devices.

SECTION II: MONITORING COVERAGE

MONITORING IMPACTS 41.7% OF ALL VULNERABILITY DISCLOSURES

To understand the impact of monitoring on vulnerability disclosures, we looked at the CVSS base metrics and vulnerabilities disclosed to date. There is a raging debate on the applicability of CVSS to medical devices, and we agree it's not perfect, but it gives a baseline from which to discuss impacts.

There are eight base metrics included in the CVSS v.3.0 guidance, and six of these are directly impacted by monitoring practices implemented at the application level (indicated in bold below):

1. **Attack Vector**
2. **Attack Complexity**
3. **Privileges Required**
4. User Interaction
5. **Scope**
6. Confidentiality Impact
7. **Integrity Impact**
8. **Availability Impact**

To be clear, we are not saying monitoring is a panacea to be relied upon in lieu of a robust security framework. Instead, we are hypothesizing that if monitoring is layered into a security program, it would have reduced the CVSS score for 41.7% of all vulnerability disclosures released and potentially decreased the need for recalls and/or urgent software updates (see Appendix A for detailed analysis).

It should also be noted that, since vulnerability disclosures are released by device vendors, they do not have the luxury of relying on any network monitoring tools HDOs may have put in place as a compensating control. Only standard, mandatory monitoring solutions implemented and maintained by the device vendors could have the potential of decreasing a vulnerability's CVSS score.

IMPACT OF MONITORING ON UNCONTROLLED VULNERABILITIES

The FDA Postmarket Cybersecurity Guidance (December 2016) cemented the idea of controlled vs. uncontrolled risk for medical devices. Uncontrolled risk is when there is a residual risk of patient harm due to inadequate compensating controls and risk mitigations. Controlled risk is the complementary concept of there being sufficiently low residual risk of patient harm as a result of a device's particular cybersecurity vulnerability.

We investigated the mitigations referenced in vulnerabilities disclosed to date to determine if vulnerabilities that would otherwise be 'uncontrolled' and potentially require a recall, could be considered 'controlled' due to monitoring practices in place. Picking two advisories with similarCVSS vector strings and similar root causes, ICSMA18-144-01 and ICSMA17-250-02A were compared. ICSMA 17-250-02A had a CVSS score of 9.8 and referred to monitoring network activity for rogue servers as part of the mitigation plan. In contrast, ICSMA 18-144-01 did not refer to any monitoring intervention, but had a lower CVSS rating of 7.5. While the CVSS scores do not reflect a reduced risk as a result of monitoring mitigations available, it is plausible that the vulnerability risk determination is substantially different for the two advisories based on the fact that additional monitoring of the pump can reduce the risk of patient harm to an acceptable level.

Unexpectedly, there were five of the 62 vulnerability advisories which recommended disabling connected functionality — with an average CVSS rating of 7.36.

ICS-CERT	Timeline Relative to FDA Guidance	CVSS Score	Vulnerability Description	CVSS Vector String
ICSMA-18-144-01	Post - FDA	7.5	An attacker with network access to the integrated web server could retrieve default or user defined credentials stored and transmitted in an insecure manner.	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
ICSMA-17-250-02A	Post - FDA	9.8	The pump with default network configuration uses hard-coded credentials to automatically establish a wireless network connection. The pump will establish a wireless network connection even if the pump is Ethernet connected and active; however, if the wireless association is established and the Ethernet cable is attached, the pump does not attach the network stack to the wireless network. In this scenario, all network traffic is instead directed over the wired Ethernet connection.	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

RELATIONSHIP BETWEEN ROOT CAUSE AND MONITORING

The root causes for vulnerabilities disclosed over the last five years were reviewed to assess how monitoring would have impacted common scenarios (see root cause definitions in Appendix B). As the FDA Premarket Guidance (October 2018) makes clear, community-wide collaboration is needed to build an effective product security program. Thus, we assessed the disclosed vulnerabilities' root causes against monitoring performed at the device, HDO or 'at-home' (i.e. in a patient's home).

Application level monitoring configured and managed at the device level would potentially be effective in 81.8% of the common scenarios assessed (see appendix C for scenarios assessed). Interventions assessed include monitoring software bill of materials for known vulnerabilities, identifying deviations in behavior from established baselines, and monitoring for failed cryptographic signature verifications.

Network monitoring within an HDO would have helped in 86.4% of the common scenarios assessed. Growing capacity of HIT staff would prove helpful in investigating flags from monitoring, but would need to be balanced against clinical alarm fatigue. However, if the HDO-level monitoring were optional, and at the direction of the HDO, it likely would not constitute a Compensating Control in the eyes of regulators, leaving the device vendor to deal with the consequences of their higher CVSS score.

The potential for an MDM to rely on a monitored network is eliminated for those devices that operate outside of an HDO. Imagine a patient's home and a device that connects to their home network. Neither an MDM nor HDO have authority to manage the home network that these 'at home' devices operate in. In isolating the vulnerabilities for devices that operate 'at home,' user authentication was the root cause 33.3% of the time (compared to 45.5% of the HDO located device vulnerabilities). It is therefore unsurprising that the common scenarios in vulnerability disclosures reviewed did not include any monitoring mitigations in a patient's 'at home' network (see Appendix C for details).

Root Cause	On Device	Both	HDO	Grand Total
Code Defect	1	6	23	30
Encryption	4	1	13	18
Misc			4	4
Operating System Vulnerability	1		7	8
System Configuration	2		13	15
Third Party Library			7	7
User Authentication	5	3	56	64
Grand Total	**13**	**10**	**123**	**146**

BUSINESS IMPACT OF MONITORING

There have been a total of seven safety communications from the FDA attributed to cybersecurity, three of which advise HDOs to implement network monitoring to mitigate the risk of these vulnerabilities being exploited. A safety communication is not a recall, but reflects current issues posing a serious patient safety threat. We believe effective device monitoring can perhaps limit the extent of MDM effort in response to these types of safety concerns.

A full-blown recall is estimated by McKinsey to cost up to $600M, while the costs associated with non-routine quality recalls (including major observations, recalls, warning letters, and consent decrees, along with associated warranties and lawsuits) are estimated to cost the industry between $2.5B - $5B annually. It is not inconceivable that monitoring devices for abnormal behavior can target MDM responses to those devices demonstrating the greatest patient safety risk.

SECTION III: OBSERVATIONS & PREDICTIONS

Location of care will influence monitoring strategies

Healthcare has been shifting outside of the HDO to accommodate increasing costs in care delivery, remote patient geography, and to accommodate populations that are unable to access an HDO on an ongoing basis. These changes have been great for patients and providers, enabling ongoing monitoring of patients even when they're not in the HDO. But it also means that some connected devices operate outside of the secured and monitored HDO network, while sending data back to providers within the HDO network. The introduction of these connection points also serve as the introduction of additional threat vectors that need to be managed. The new regulatory requirements around intrusion detection require device-based monitoring to be standard in newly designed "at home" medical devices.

Threat sharing can improve with third party partnership

Empirically seen to be beneficial, and mandated by the FDA, threat sharing across the industry would welcome a level of maturity that has yet to be seen. As noted in our previous whitepaper, only seven of the top 37 device vendors have disclosed even a single vulnerability. There are many possible reasons other top vendors have yet to disclose a vulnerability, including the logistical challenges of cooperative vulnerability disclosures, identifying and sharing engineering technical details to enable other manufacturers to avoid similar mistakes, fear of legal ramifications, and the difficulty of completing all of this in a timely fashion. Using a third-party to perform monitoring of device meta-data will become an increasingly popular approach for MDMs.

Number of disclosures will increase

Security researchers are credited on 43% of these vulnerabilities, which anecdotally is lower than other industries. This could be attributed to how difficult it is to source medical devices. Collaborative threat-sharing by device vendors, mandated by the FDA, is moving in the right direction, but does not seem to keep pace with the manifestation of risks.

Taking this in conjunction with an assessment showing disclosed vulnerabilities arose from only 12% of the NIST-CSF subcategories (see Appendix D), seems to indicate a large number of vulnerabilities have not been disclosed. There are two possible explanations for this:

- There have not been any vulnerabilities associated with 98 of the subcategories included in the NIST-CSF guidance
- Vulnerabilities with 98 of the 108 subcategories have yet to be reported or identified for medical devices

The truth likely lies somewhere between the two, but as the researcher community is increasingly engaged the number of vulnerability disclosures is bound to increase.

[2] C. Kamhoua, A. Martin, D. K. Tosh, K. A. Kwiat, C. Heitzenrater and S. Sengupta, "Cyber-Threats Information Sharing in Cloud Computing: A Game Theoretic Approach," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, 2015, pp. 382-389.

DISCLOSURES

The authors of this paper are employed by MedCrypt Inc., a medical device cybersecurity software developer.

Thank you.
Mike Kijewski, CEO
mike@medcrypt.co

APPENDIX A

DECREASE IN CVSS MEAN

The applicability of monitoring to CVSS metrics is assessed in the table below, with particular emphasis on how monitoring at either the device or HDO would impact CVSS values.

CVSS Metric (values)	Definition	Impact of Monitoring	Impact by Numbers
Attack Vector (physical, local, adjacent, network)	Context by which vulnerability exploitation is possible	• Application monitoring could detect L, A & N attacks • Network monitoring can detect network based attack vectors	• Application layer monitoring - 88.5% • Network layer monitoring - 50.4%
Attack Complexity (high, low)	Conditions beyond attackers control that must exist to exploit a vulnerability	• Application monitoring could detect repeated exploitation across the same component • Network monitoring could detect the highly complex man in the middle attack	35/46 high complexity attacks may have been detected with application and/or network monitoring in place
Privileges Required (none, low, high)	Level of authorization needed before an exploitation occurs	Application monitoring could identify authentication patterns abnormal to baseline behavior	69% of vulnerabilities had no privileges required, indicating abnormal pattern identification may be effective
User Interaction (none, required)	Requirement for a user, other than the attacker, to participate in the successful compromise of a component	• Application monitoring could identify authentication patterns abnormal to baseline behavior • Network monitoring could identify user activity with external domain	70.2% of vulnerabilities need no user interaction, indicating traditional user monitoring may not be effective
Scope (changed, unchanged)	The ability for a vulnerability in one software component to impact resources beyond its means, or privilege	A combination of network and application monitoring would be helpful to see if abnormal requests across software components occur	Scope change was seen in 16.8% of vulnerabilities disclosed, with an average rating of 7.64
Confidentiality Impact (high, low, none)	Whether access and disclosures of data was shared to unauthorized users	Monitoring is unlikely to have an impact on the loss of confidentiality due to a vulnerability	
Integrity Impact (high, low, none)	Impact to veracity of information	Application monitoring can ensure changes to critical/sensitive data is identified when not coming from an authenticated source	Unsurprisingly, only ~15% of vulnerability disclosures rated low integrity impact, implying most data included in a vulnerability is sensitive
Availability Impact (high, low, none)	Loss of availability of the component itself	Both network and application monitoring would determine if a component is unavailable	65% of vulnerabilities had an availability impact, suggesting the utility of hacking a device may be availability vs. data

APPENDIX B

DESCRIPTION OF VULNERABILITY CAUSE CATEGORIES

CVSS V3 Ratings:	Can be described as imperfect implementations of otherwise secure software designs. An example of a code defect would be a Buffer Overflow, Many of these defects can be identified in the verification and validation process using tools like Static Code Analysis and Fuzz Testing.
Encryption:	The lack of encryption of sensitive data, or vulnerabilities in the way this encryption is implemented, can leave devices and data vulnerable to attack. Common examples are storing user credentials in plain text, storing encryption keys in an insecure fashion, or vulnerabilities discovered in the underlying encryption software and algorithms.
Operating System Vulnerability:	Many medical devices include computers running retail operating systems, like Microsoft Windows. These operating systems are regularly found to have vulnerabilities unrelated to the medical device itself, but that can affect the function of the device if left unpatched. One example would be the March 2017 "EternalBlue" vulnerability in Microsoft Windows handling of SMB transactions.
User Authentication:	Failure to require user authentication for critical functions, or vulnerabilities in the way users are authenticated, can leave devices susceptible to attack. One common example is the use of "hard-coded" user credentials used across a fleet of devices.
System Configuration:	Connected medical devices and their underlying software systems can be designed "securely", but configured in a way that leaves a device susceptible to attack. A common example is failing to disable unnecessary OS services and block all unused ports.
Third Party Library:	Medical devices frequently rely on third party software for critical functions, which can be found to have vulnerabilities. One example would be a medical device including a version of a database server application found to have a publicly disclosed vulnerability.
Miscellaneous:	Disclosures that did not fit into one of the above categories were labeled "Miscellaneous."

APPENDIX C

CODE DEFECT

Common Scenarios Identified in Vulnerabilities Disclosed to Date	Impact of Device Based Monitoring	Impact of Monitoring At HDO
Denial of service as a result of: **• out-of-bounds read** **• overflow of TCP packets**	Anomalous device behavior could be identified through application layer monitoring	Network monitoring could be used to identify the absence of responses to service requests
Buffer overflow	Application layer monitoring of device behavior deviations (in this case 18 out of 31 vulnerabilities)	
Inadequate session expiration parameter	Application monitoring for anomalous session durations	Network monitoring for anomalous session durations
Inappropriately restricted "RF wake-up" commands	Application monitoring for anomalous session frequency	Network monitoring for anomalous session frequency

ENCRYPTION

Common Scenarios Identified in Vulnerabilities Disclosed to Date	Impact of Device Based Monitoring	Impact of Monitoring At HDO
Transmitting data in plain text	Monitoring at application layer for the absence of encrypted communication	Network monitoring for plain text
Hard coded cryptographic keys	Anomalous device behavior identified at the application	Anomalous device behavior identified at the network layer
Private keys and certificates are stored on the device in cleartext		Monitoring SSL traffic
Sensitive data at rest is not encrypted	Monitoring at application layer for the absence of encrypted communication	Monitoring SSL traffic

OPERATING SYSTEM VULNERABILITY

Common Scenarios Identified in Vulnerabilities Disclosed to Date	Impact of Device Based Monitoring	Impact of Monitoring At HDO
Hard-coded operating system passwords		Anti-virus monitoring can be an effective tool for identifying known malware is present
Outdated anti-virus signatures	Inclusion of operating system attributes in a CBOM being monitored for CVE vulnerability relevance	

SYSTEM CONFIGURATION

Common Scenarios Identified in Vulnerabilities Disclosed to Date	Impact of Device Based Monitoring	Impact of Monitoring At HDO
Debug functionality being exploited		Network monitoring for anomalous traffic
Unauthorized uploads being allowed	Monitoring for update signature verification	
Vulnerability in software update mechanism		
Vulnerabilities by common ports		Network monitoring for port vulnerabilities

THIRD PARTY LIBRARIES

Common Scenarios Identified in Vulnerabilities Disclosed to Date	Impact of Device Based Monitoring	Impact of Monitoring At HDO
Exploitable known vulnerabilities in the device version of a third party library	Monitoring CBOM components	Monitoring CBOM components to inform network segmentation
Denial of service as a result of out-of-bounds read	Anomalous device behavior identified at the application	Network monitoring could be used to identify the absence of responses to service requests
Buffer overflow	Application layer monitoring of device behavior deviations	

USER AUTHENTICATION

Common Scenarios Identified in Vulnerabilities Disclosed to Date	Impact of Device Based Monitoring	Impact of Monitoring At HDO
Hard-coded credentials • username • password • cryptographic keys	Monitoring application layer for abnormal authentication behavior	Monitoring network for abnormal connectivity patterns
Credentials stored in cleartext		
Not validating host certificates		
FTP connectivity		
Default credentials that cannot be changed	Monitor application layer for default account login	Monitor default account logins

APPENDIX D

The data extracted from the ICS-CERT Advisory Database, including details on advisories and MedCrypt coverage are found here and is summarized in the table below. Assuming a normal distribution of NIST-subcategories across medical device vulnerabilities, it is then surprising to see only 12% of NIST-subcategories included in any medical device vulnerability to date.

NIST-CSF Subcategory	Oct 1, 2013 - Dec 28, 2016	Dec 29, 2016 - March 31, 2019	How MedCrypt would have helped
None Noted	1		Detective monitoring of anomalous elevated access
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed		1	Detective monitoring of a device connects to a different access point
DE.CM-1: The network is monitored to detect potential cybersecurity events		3	Metadata monitoring to identify deviations from normal behavior
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events			
DE.CM-4: Malicious code is detected	2	3	Port monitoring and encryption on communications inhibit devious updates from being installed
DE.CM-5: Unauthorized mobile code is detected			
ID.RA-3: Threats, both internal and external, are identified and documented	1	2	Code vulnerabilities are diminished through layered security in communication encryption
PR.DS-1: Data-at-rest is protected	3	6	Encryption of data through MedCrypt library
PR.DS-2: Data-in-transit is protected	7	7	Encryption of data through MedCrypt library
PR.DS-4: Adequate capacity to ensure availability is maintained	2	13	Excessive capacity constraints beyond normal behavior are identified through monitoring
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	4	10	Keys issued using MedCrypt restrict endpoint communication
PR.AC-2: Physical access to assets is managed and protected			
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	1	4	Architecting limited endpoint communication
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi- factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	15	46	Key provisioning and management for endpoints
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. c oncept of least functionality)	8	13	Monitoring and alerting based on deviations in endpoint behavior
PR.PT-2: Removable media is protected and its use restricted according to policy		1	Modified code injection through removable media would be detected by monitoring
PR.PT-4: Communications and control networks are protected		5	Unintended connectivity to VPN would be identified through monitoring