

Transforming Clinical Asset Management & Security

Keeping Devices Secure and Patients Safe

The exploding number of medical and IoT devices make it difficult for healthcare delivery organizations to manage and secure everything in their clinical network. Anything that is not actively managed by the healthcare organization adds costs and risks to the environment, which ultimately compromises the safety of sensitive data and patient care. To protect their resources and operations, healthcare organizations need to accurately identify all the devices in their network and take measures to proactively manage and mitigate any risks they may pose.

Unfortunately, medical devices are not like other devices, which means general discovery and mitigation tactics don't necessarily apply or work. It takes deep clinical expertise to be able to identify different devices and understand the role they play in clinical workflows and patient care to establish safe, secure policies and remediation actions. Medigate and TRIMEDX have that clinical expertise and practical know-how.

Both have applied their clinical engineering proficiency to build solutions that address the specific management and security needs of healthcare delivery organizations. They have come together in a partnership to deliver a technology-enabled solution that supports a healthcare organization's capital planning, IT and security initiatives. Together, Medigate and TRIMEDX ensure hospitals have efficient, effective clinical asset management and a strong cybersecurity stance.

The Medigate – TRIMEDX Solution

TRIMEDX and Medigate deliver an integrated solution that merges the TRIMEDX CAM Advanced and CYBER Advanced solutions with Medigate's real-time visibility, utilization data and threat/vulnerability detection. Medigate's Device Security and Asset Management Platform integrates with TRIMEDX's proprietary clinical CMMS platform, RSQ, to provide a dynamic solution that gives healthcare organizations comprehensive visibility into all the devices in their environment and proactive risk mitigation capabilities to keep data and patients safe.

By combining Medigate's deep data analysis and cybersecurity expertise with TRIMEDX's vast clinical network and know-how, healthcare organizations can be confident they have what they need to:

- Maintain a comprehensive inventory of all connected devices in their clinical network
- Conduct real-time monitoring of connected medical devices
- Gain insights into clinical asset vulnerabilities to support proactive risk mitigation
- Identify abnormalities and threats in the network
- Accelerate responses to risks, including sequestering devices and applying patches

How the Solution Works

The Medigate Platform continuously monitors the network, using deep packet inspection (DPI) to provide a real-time inventory of all the medical and IoT devices connecting to the network. Medigate feeds the device information into TRIMEDX RSQ, including device details, such as manufacturer, make, model, operating system (OS), embedded software, and protocols, as well as location and utilization information. Medigate also analyzes device and network communications, as well as medical protocols and workflow patterns, to accurately detect anomalous behavior and identify threats in real time.

TRIMEDX leverages this data in the CAM Advanced solution in its unique CYBER Risk scoring algorithm to derive a cybersecurity risk score for each individual clinical asset. This risk score, along with the aggregated device utilization data provided by Medigate and TRIMEDX's national asset benchmarking data, is used to generate the proprietary TRIMEDX replacement, upgrade, disposition and reallocation (RUDR) Score. This score helps health systems optimize their clinical asset inventories, providing actionable recommendations to streamline their clinical asset management and reduce risk.

As part of the CYBER Advanced solution, a dedicated TRIMEDX team utilizes the Medigate network monitoring data to proactively identify cyber vulnerabilities and advocate with OEMs to acquire OEM-validated patches. The TRIMEDX CYBER Academy trained CYBER specialists then manage all aspects of cybersecurity remediation.

Clinical Asset Management Use Case

RUDR SCORE™

By incorporating Medigate's visibility, cybersecurity risk data and utilization information on all the connected devices in the clinical network, along with TRIMEDX national benchmarking data, the CAM Advanced solution helps healthcare organizations optimize their clinical asset inventory. Through the application of the proprietary TRIMEDX RUDR Score, health systems can enhance their capital planning to:

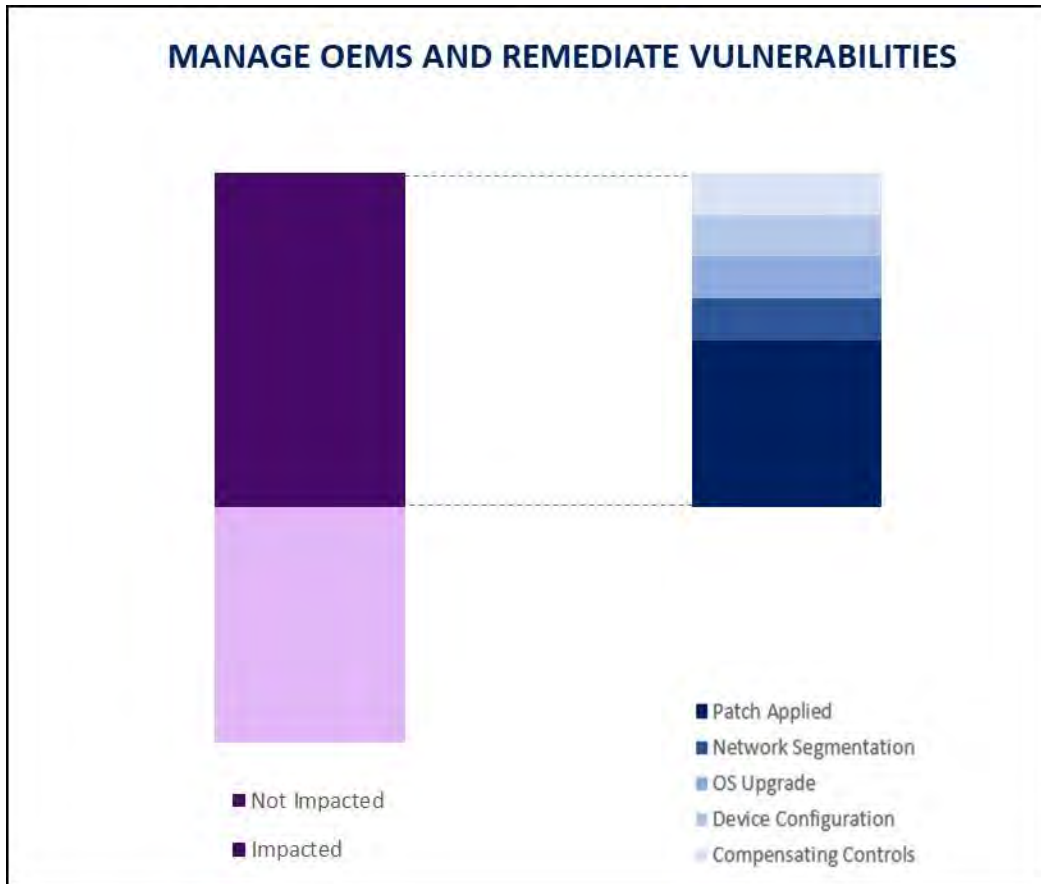
- Reduce and defer CapEx and OpEx investments with strategic replacement planning
- Defer CapEx investments through targeted clinical asset upgrades
- Monetize the true market value of used clinical assets through disposition
- Save CapEx through strategic reallocation of excess clinical asset inventory to alternate sites

In addition, by using the Medigate device utilization data to identify when to schedule maintenance, health systems are able to extend the useful life of their clinical assets by an average of 30% above national standards.

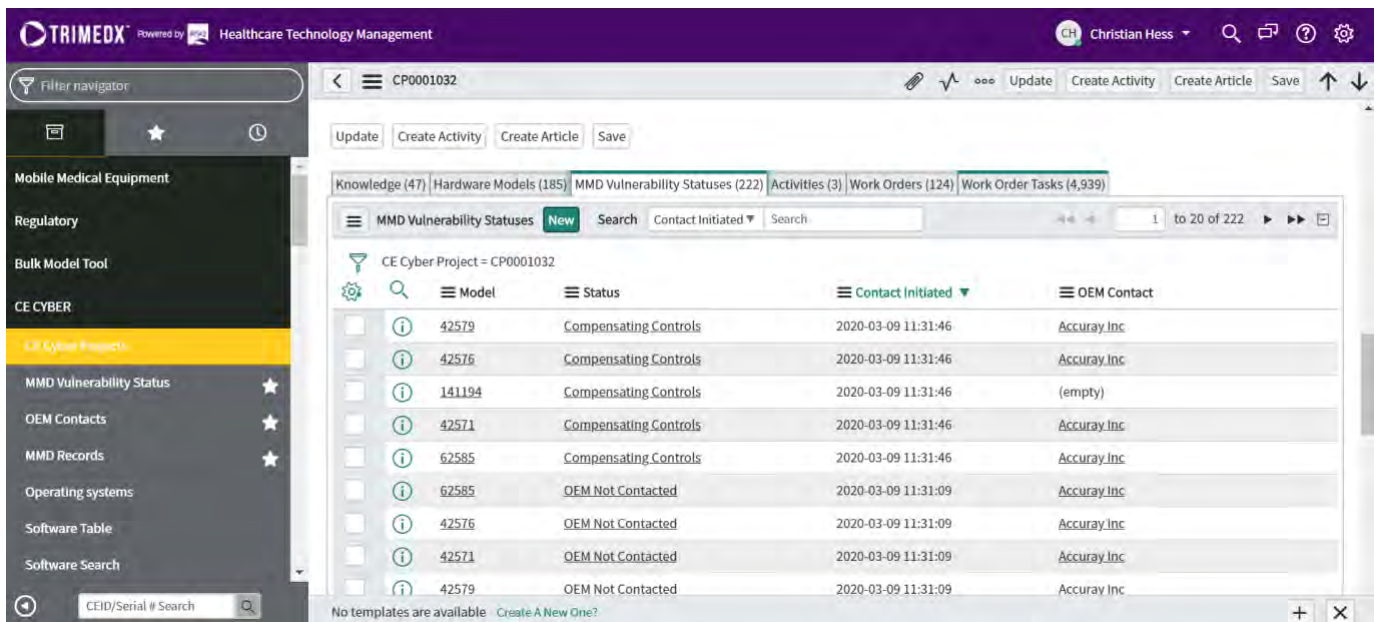
Risk Management Use Case

The real-time detailed device information that Medigate provides helps TRIMEDX build out effective patch management and risk abatement strategies. For example, if a vulnerability is announced, Medigate will identify which devices are affected, where they are located and whether there are any available patches or updates. A ticket will then be opened to notify TRIMEDX to take the appropriate measures to mitigate the risks created by the vulnerability. Ultimately, TRIMEDX will manage the installation of the patch (when available) to close out the ticket and mitigate any chance of exploit.

There are a number of ways that healthcare organizations can understand and track the impact of a vulnerability in their environment and the progress of its remediation. For starters, TRIMEDX provides macro information on patching cycles through its dashboard.



TRIMEDX also enables healthcare organizations to easily drill into the details of activities surrounding specific vulnerabilities.



Additional Visibility

TRIMEDX helps health systems prioritize cyber projects based on the proprietary CYBER Risk Score of each device. Details collected by both Medigate and TRIMEDX are used to complete the assessment and produce the CYBER Risk Score, which can be used to make decisions around how best to protect the healthcare organization's dynamic environment. The CYBER Risk Score incorporates information on the:

- **Device**
 - Operating System
 - Vulnerabilities (known and/or open)
 - Outdated firmware
 - Installed anti-virus protection
 - Storing of ePHI information
- **Network**
 - Connection type (wired/wireless)
 - Network topology
 - Internet communication
 - Transmission of ePHI
- **Severity**
 - Class of device
 - Risk to patient safety / consequence of failure
 - Likelihood of exploit
 - Proprietary TRIMEDX AEM Risk Score



Healthcare organizations can also take advantage of the TRIMEDX Supplier Scorecard to better understand how each manufacturer is responding to their risks. The Scorecard pulls information from both Medigate and TRIMEDX to provide real-time insight into each manufacturer's:

- Open vulnerabilities
- Devices impacted
- Unique models impacted
- Models that will not be patched
- Models for which the OEM has not responded
- Models for which a patch has either been issued or is in development
- Average response time

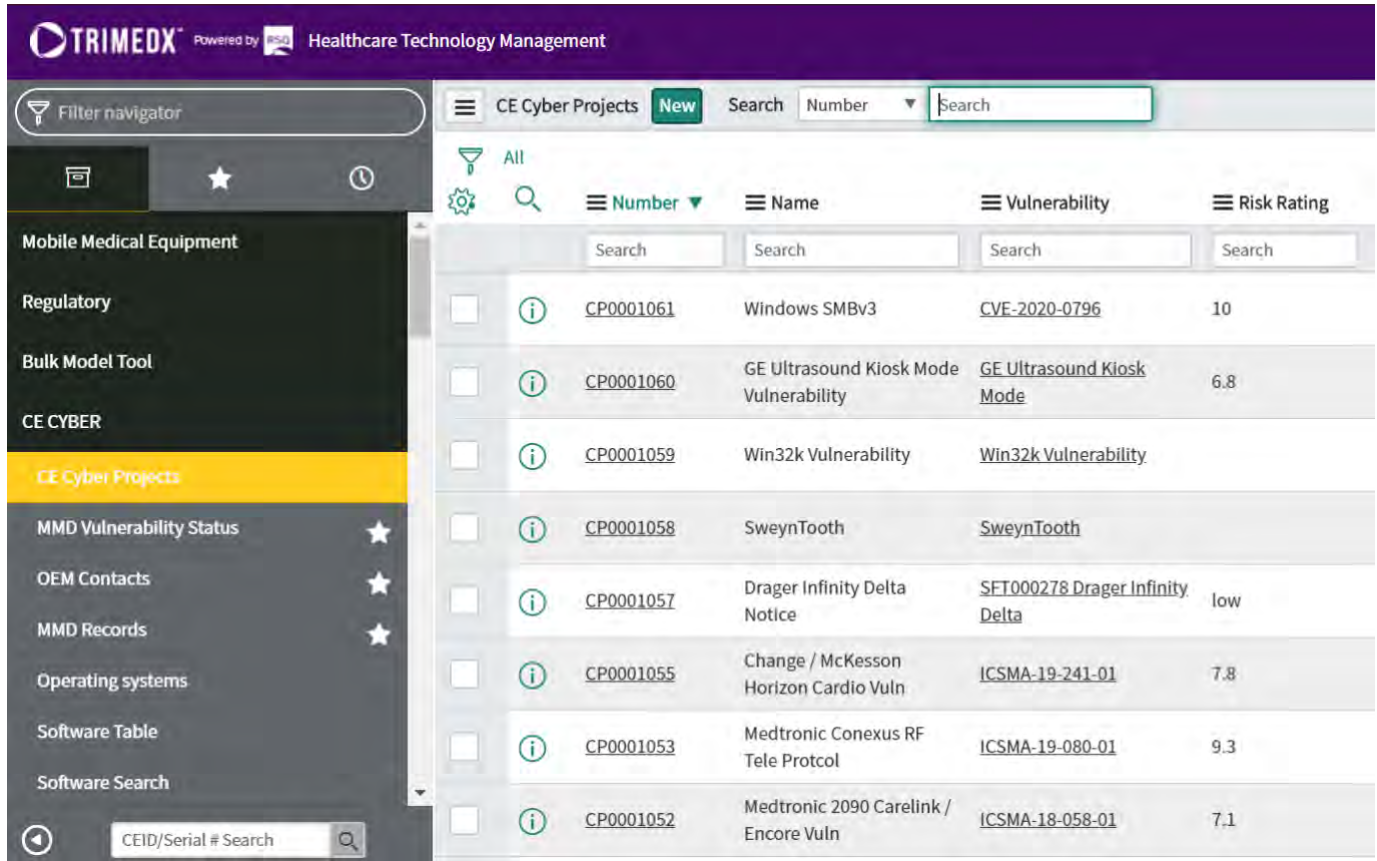


Detection and Prevention Use Case

Medigate can continuously monitor and analyze the healthcare organization's network traffic to identify anomalous device behaviors, based on activity that deviates from network and device protocols, as well as expected clinical workflows and manufacturer-intended functionality. Medigate will alert TRIMEDX on the risk, opening a ticket and providing precise incident information that enables immediate action to be taken to mitigate the threat, including quarantining the device or restricting Internet access.

Anomalous Event Detection						
CEID	OEM	Model	Description	Issue	Recorded	
56166519	Systemex	XT1800	Cath Lab Workstation	Anomalous Network Activity	1/27/20 7:12 AM	
96804264	McKesson	Z400	PACS Workstation	Unremediated Vulnerability Opened	1/26/20 2:24 PM	
40100942	Philips	PIIC IX	Central Monitor Station	Unsupported OS Installed	1/24/20 12:00 PM	

TRIMEDX can manage the entire process to ensure the threat is appropriately addressed, while providing the healthcare organization visibility into every step:



Redefining Clinical Asset Management & Security

The Medigate – TRIMEDX partnership brings healthcare organizations an asset management and security solution, anchored by clinical engineering tenants and a focus to serve the healthcare community exclusively. Together, they bring clinical expertise and cybersecurity know-how to provide healthcare organizations the visibility, management and remediation capabilities they need to improve management efficiencies, mitigate risks and keep patients safe.

For more information or to discuss how you can benefit from the Medigate – TRIMEDX solution, please schedule here.