Ensuring Uninterrupted Operations of Connected Medical Devices

Healthcare organizations continue to evolve, adopting the latest technology to provide the best and uninterrupted care. The advancement in medical devices is one such example where the devices are increasingly being networked to provide efficient operation and management. As it had been in the past, it is the responsibility of the clinical engineers to ensure continued availability and operations of these connected medical devices as they continue to evolve.

Unfortunately, many tools and processes that clinical engineers have come to depend on have not kept pace or are no longer adequate. Traditional processes such as the use of static inventory database, manual room-to-room device audits, and time-based device maintenance plans are severely limiting clinical engineers' ability to efficiently manage and ensure the uninterrupted availability of connected medical devices. With increasing networking footprint, clinical engineers must now coordinate with Information Technology (IT) departments to ensure proper network configuration and segmentation for connected medical devices.

The most recent challenge introduced by connected medical devices is the rise in cyberattacks. Increasing number of cyberattacks now aim to disrupt healthcare organization's ability to provide care by targeting connected medical devices. To make the matters worse, many medical devices cannot be easily patched and clinical engineers must abide by various requirements from agencies such as the FDA.

The Challenges

REACTIVE WORK MODEL – Current processes and work models are based on responding to incidents. Without the tools to proactively manage and maintain devices, clinical engineers can only strive to improve their reaction time rather than reducing the number of incidents.

REAL-TIME DEVICE INVENTORY – Clinical engineers often lack the accurate inventory of devices deployed. Often relying on spreadsheets and static databases, clinical engineers cannot adequately plan for outages or spare devices.

DEVICE INSIGHT – Connected medical devices are essentially black boxes. The inner workings such as the underlying OS and applications are hidden from clinical engineers making it difficult to assess the device risk and vulnerabilities.

DEVICE UTILIZATION METRICS – Device utilization data are often not available, forcing clinical engineers to schedule maintenance based solely on time-based intervals and limiting effective deployment of devices where it can best be utilized.

SUPPORT FROM DEVICE MANUFACTURER – Many connected medical devices are designed to be in operations for years and in some cases, decades in its original design. Receiving assistance to patch or upgrade devices from the device manufacturer is uncommon.

The only solution to leverage device personality via deep learning & AI

Zingbox IoT Guardian enables clinical engineers to efficiently manage and maintain connected medical devices. It is the first and only solution to leverage the individual personalities of connected medical devices to provide accurate device visibility, protection and optimization. IoT Guardian leverages deep learning and Artificial Intelligence (AI) to identify, classify, and profile each connected medical device. The integration with ticketing and other infrastructure enables the same AI to proactively generate work-orders for clinical engineers to stay a step ahead of device failure and service disruptions.

VISIBILITY – Critical insight required by all clinical engineers is the accurate and real-time visibility into the inventory of connected medical devices. Zingbox IoT Guardian automatically discovers all connected medical devices on the network, identifies them, and categorizes them into respective types. New devices are detected as they come online in real-time and integration with popular Computerized Maintenance Management Software (CMMS) solutions ensure always up-to-date device inventory.

SECURITY – Rather than reacting to the malware, IoT Guardian focuses on what all clinical engineers care about, ensuring connected medical devices behave as they were intended. Zingbox IoT Guardian profiles individual connected medical devices to develop their unique personalities. The personalities are then assessed for deviations from their historical norm as well as the baselines across similar device types.

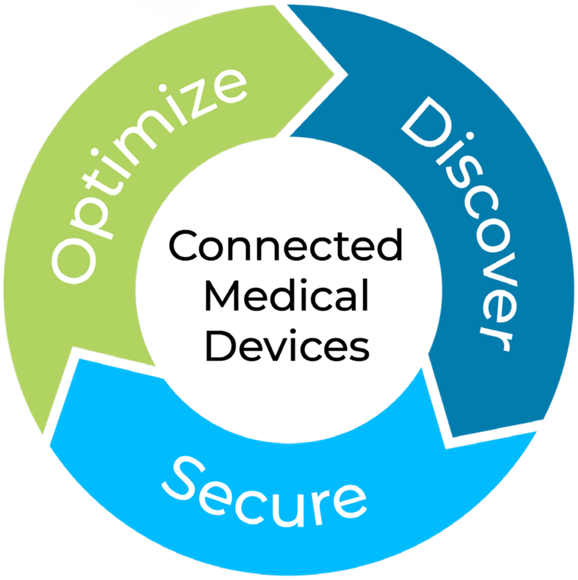
OPERATIONAL INTELLIGENCE – Without insights into device utilization, clinical engineers are forced to manage and maintain their connected medical devices on a fixed time interval. Zingbox IoT Guardian removes this ambiguity, enabling clinical engineers to adopt Alternate Equipment Maintenance (AEM) programs and efficiently manage devices based on actual usage. For the first time, clinical engineers can proactively manage connected medical devices rather than simply reacting to trouble tickets or incidents.

The Benefits

Zingbox IoT Guardian enables clinical engineers to:

- Discover all networked connected medical devices
- Classify devices into categories
- Provide device utilization and operational insights
- Minimize maintenance and lower TCO
- Identify risks for each connected device
- Receive real-time alerts on anomalous device behavior
- Real-time inventory update of popular CMMS solution
- Maintain business continuity

Even with the advancements in medical devices, clinical engineer's charter remains the same; ensure uninterrupted device operations. Zingbox enable clinical engineers to address their increasing responsibilities with a modern solution designed from the ground-up for connected medical devices.



About Zingbox

Zingbox IoT Guardian is an Internet of Things security solution that provides visibility into and protection for enterprise IoT assets against cyber and insider threats. A **non-intrusive, agent-less, signature-less** solution, IoT Guardian uses machine learning for asset discovery, risk assessment, baselining the normal behavior of devices, and discovery of threats. Zingbox was founded by Silicon Valley IT industry leaders and experts in networking, big data, IoT and security.