Zingbox

AIMS®

SOLUTION BRIEF

Bolster Your Healthcare CMMS with Cybersecurity

KEY BENEFITS

- Discovery and classification of medical devices
- Risk rating for each IoT device
- Alert upon detection of anomalous device behaviors
- Security event triggered clinical work orders
- Auto assignment of work orders to appropriate technicians
- Asset and security analytics on a single pane of glass
- Granular security analysis based on device make, model, and version

Many healthcare organizations rely on Computerized Maintenance Management Systems (CMMS) to house critical information on assets, work orders, maintenance schedules as well as manage the overall workflow. While CMMS addresses many of the operations and management needs, clinical engineers and IT are increasingly challenged to protect the connected medical devices from modern hackers and the latest malware/ransomware. Legacy security solutions designed to secure PCs and servers with no context of connected medical devices have yielded limited success. Their lack of integration with CMMS solutions also requires manual correlation between two disparate systems. This requires additional resources and results in slower reaction time.

An ideal solution for healthcare organizations is one composed of Internet of Things (IoT) security designed from the ground up to protect connected medical devices from the latest threats. It would leverage machine learning to discover, assess risk, baseline normal behavior, and detect anomalous activities of connected medical devices. The same security solution would be integrated with the CMMS to provide richer device security analytics, as well as correlate device vulnerability and security with asset management, workflow, and other operation and management capabilities. Such a solution is now possible with the integration between AIMS and Zingbox.

AIMS and Zingbox Integration

The integration of AIMS and Zingbox provides unparalleled device visibility by combining device context from the CMMS with the security analytics from IoT security. It also integrates security intelligence into clinical engineering workflows. Key benefits include:

SECURITY REMEDIATION – Security event triggered clinical work orders

RAPID INCIDENT RESPONSE – Auto assignment of work orders to appropriate technicians

SINGLE PANE OF GLASS – Asset information and security analytics available on a single pane of glass

MEDICAL DEVICE CONTEXT – Granular security analysis based on device make, model, and software version

About Phoenix Data Systems, Inc.

Phoenix is the trusted provider of the CMMS software, AIMS (Asset Information Management System), for thousands of users around the world. Phoenix was formed in the early days of specialized software based on the urgent need for hospitals to have a modern maintenance work order system. Today, AIMS is used in 3,000 facilities in 18 countries. Phoenix is now developing its fifth platform change and designing software to carry AIMS users well into the early 2020's and beyond.

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.