ZingBox

White Paper

IoT Guardian for the Healthcare Industry

Introduction

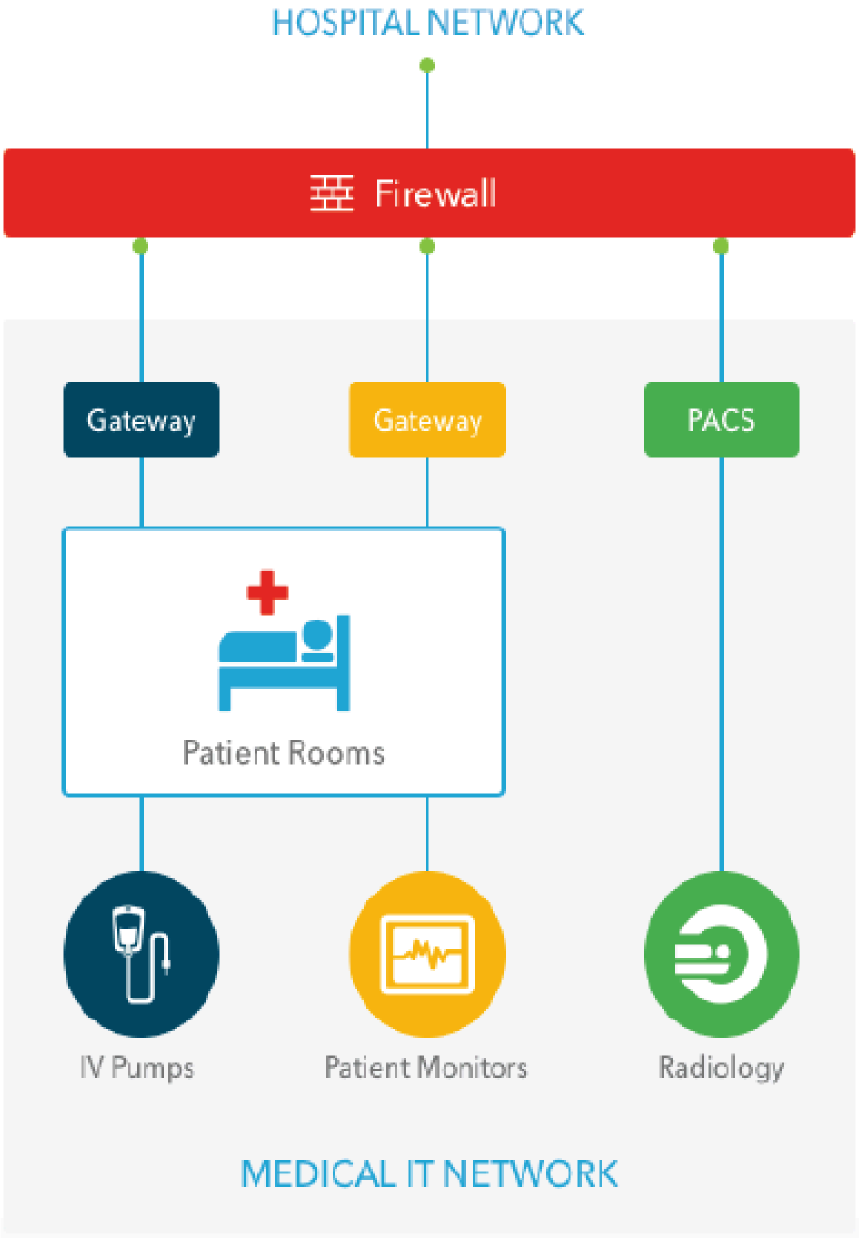
In 2015, Healthcare was the most attacked industry. In fact 90% of hospitals reported they had been targeted by cybercriminals in the past two years. Of these documented attacks, 17% were facilitated by Internet-connected (IoT) medical devices. Consequently, if a hospital doesn't know how many connected medical devices it has, then it probably doesn't know how vulnerable it is to a cyber-attack. And we know IoT devices, designed for medical use or otherwise, are very vulnerable.

Unfortunately, the manufacturers of most Internet-connected medical devices, which includes infusion pumps, MRI machines, x-ray machines, glucose meters, heart monitors, blood gas analyzers, and more, consider cyber security as an afterthought. Little wonder that security researchers are finding that medical devices are riddled with malware that allows for them to be misused by cybercriminals in so many different ways, including providing a portal for lateral movement inside the hospital's network.

IT security experts agree that medical devices are the weakest link in a healthcare facility's network. When they are compromised, patient's health, safety, and privacy are definitely at risk.

According to Brian Selfridge at a Health Care Compliance Association webinar, “Medical devices have become an open door to the healthcare environment by virtue of the relatively lax security posture” of hospitals and the medical device manufacturing industry.

Medical Devices – Security is Overlooked



HOSPITAL NETWORK

Firewall

Gateway

Gateway

PACS

Patient Rooms

IV Pumps

Patient Monitors

Radiology

MEDICAL IT NETWORK

Firewall - the single line of defense
(With no device context only work at IP level)

Unmonitored network
(Medical IT network remains unprotected)

Lack of endpoint visibility & security
(Agent cannot be deployed)

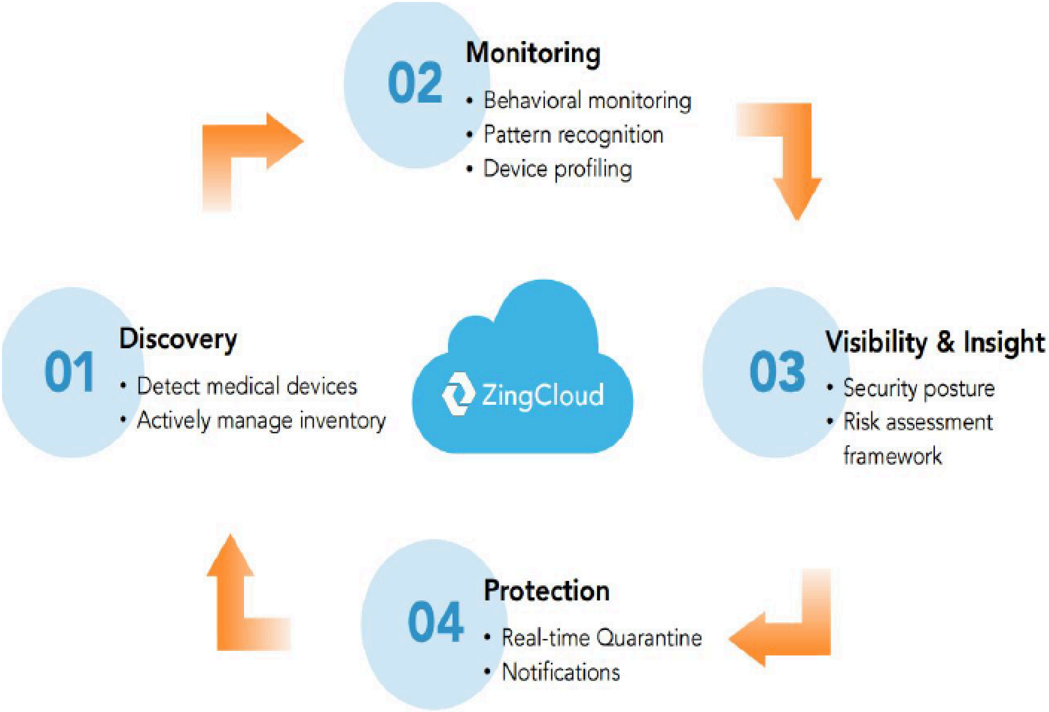
Why Traditional IT Security for Medical Devices Fails

In the past, hospital networks were homogeneous and the approach to securing them was monolithic and reactive. The behaviors of known malware, based on manual research, were described in heuristic rules and signatures that were leveraged for detection and quarantine. As healthcare facility networks have become more heterogeneous with a variety of unique connected medical devices and specific-purpose hardware, the traditional reactive approach to securing the diverse set of devices (as well as the network) is not effective – particularly when there is unique malware for each IoT device.

Traditional IT security solutions weren't designed to protect heterogeneous medical devices that have a wide variety of hardware, operating systems, and software applications. The old signature-based security at the endpoint or the perimeter fails to protect such diverse infrastructures, and a new kind of protection is needed to secure them.

IoT Guardian - The ZingBox Solution

ZingBox IoT Guardian is based on a machine learning approach that discovers, identifies and classifies connected medical devices. ZingBox then establishes a baseline of a device's normal behaviors to detect any deviations and determines if they are compromised.



The machine learning approach is a four-step process that starts with **DISCOVERY** and answering the first and most important question: “How many and what types of IoT medical devices does your organization have?” IoT Guardian is device vendor-agnostic and automatically discovers and identifies connected medical devices on the network and provides real-time operational status.

The second step in the process is **MONITORING**, which is based upon tracking device behavior, pattern recognition, and device profiling. The third step is **VISIBILITY & INSIGHT**. In this phase of the process, the ZingBox solution applies risk assessment framework to summarize the overall security posture and risk factors. The fourth and final step is **PROTECTION**, where IoT Guardian provides real-time quarantining of threats and sends notifications to the network administrators.

In summary, IoT Guardian identifies connected medical devices; detects cyber and insider threats in real time using machine-learning algorithms that spot anomalies and zero-day threats; and follows up with rapid enforcement to contain the threats.

Improving on Compliance

As new regulatory standards are being developed to cover medical devices, it has never been more critical to balance the priorities of safety and effectiveness of care. In addition to improved visibility and security, IoT Guardian uses continuous monitoring for enhancing operational and regulatory compliance. By providing compliance data and reports, ZingBox allows healthcare facilities to apply risk management techniques to medical device networks.

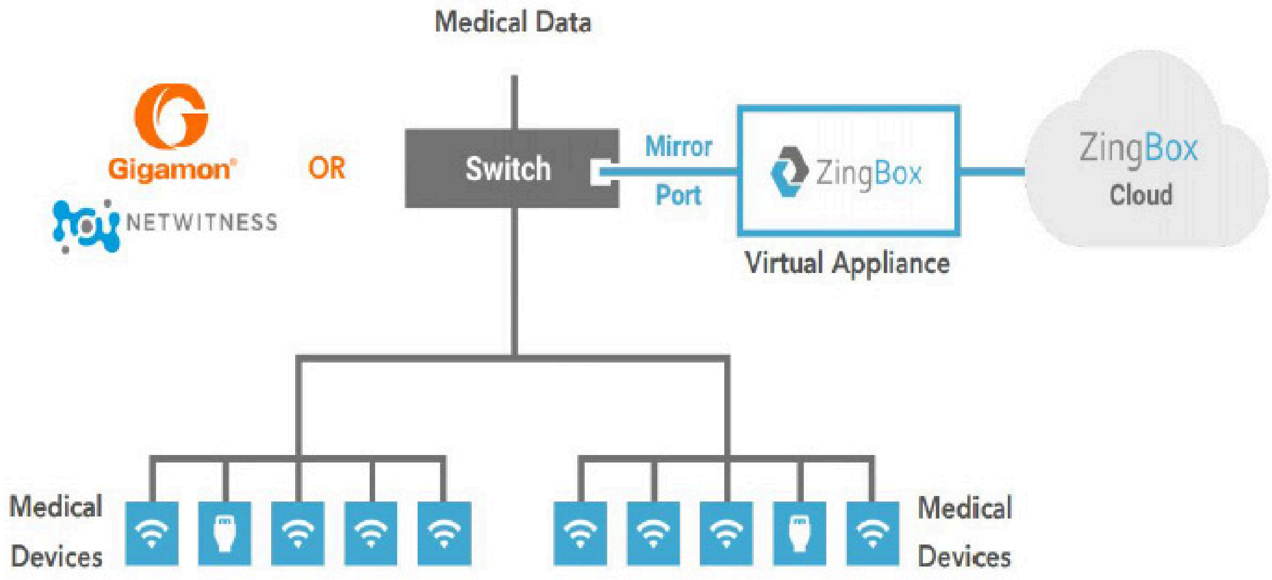
Healthcare organizations will need solutions like IoT Guardian that come with unrivaled visibility into IoT infrastructures to reveal vulnerabilities and hidden threats. This is particularly important as the U.S. Department of Health and Human Services (HSS) Office of Inspector General (OIG) ramps up security audits that include medical devices.

IoT Guardian Deployment Model

IoT Guardian offers a very flexible deployment model, and easily integrates with the existing security infrastructure. It is a non-disruptive, passive, and out-of-band deployment that does not interrupt the operation of connected medical devices to ensure operational continuity. It is made up of two components: ZingBox Inspector and ZingBox Cloud.

ZingBox Inspector is a virtual appliance that sits on premises but as an offline module. Its job is to process the network traffic from connected medical devices. It extracts insights from the network traffic and relays the meta-data (not the payload itself, but the analysis of the payload) to ZingBox Cloud.

ZingBox Cloud analyzes the meta-data and applies machine learning algorithms to discover, classify and baseline the behaviors of each device on the network. It employs advanced anomaly detection to detect deviations from baseline and seamlessly integrates with existing enterprise security controls; providing real-time policy enforcement. It also generates IoT logs and can send it to a SIEM (Security Information and Event Management) for enhanced correlation of threat vectors. ZingBox can make SIEM deployments IoT aware.



IoT Guardian Benefits

Benefits for IT Department:

- Discovery and visibility of network connected medical devices
- Agent-less, signature-less, proactive security
- Context-aware policy enforcement (policies for group of devices based on their functions)

Benefits for Biomedical Engineering:

- Medical device inventory tracking
- Operational monitoring
- Regulatory compliance

Pricing Model

ZingBox IoT Guardian is made available via a subscription-based pricing model:

- Medical device discovery and visibility
- Risk assessment and threat detection
- Policy enforcement and Integrations with other security products
- Extended data retention for compliance

Summary

To fully secure medical devices and a healthcare organization's IoT network, a new kind of solution is required, like the one developed by ZingBox. Using machine learning and other innovative technologies, the ZingBox IoT Guardian security solution provides you with unparalleled visibility into your organization's IoT infrastructure. It will reveal existing vulnerabilities and hidden threats, so you can employ context-aware policies protecting your healthcare organization from a potentially life-threatening cyberattack.

To learn more, please visit ZingBox's website at **www.zingbox.com**.

About ZingBox

ZingBox is an enterprise Internet of Things (IoT) security provider. ZingBox's IoT Guardian is a cloud-based, out-of-band solution that provides real-time visibility of and security for IoT assets. Recently named one of Silicon Valley's **hottest security startups** by *NetworkWorld*, ZingBox currently has successful deployments with a number of Fortune 500 multi-national corporations and multiple healthcare facilities.

ZingBox

Connected Medical Device Security

NETWORKWORLD
FROM IDG

Silicon Valley's
hottest security startup

465 Fairchild Drive #209
Mountain View, CA USA 94043

+1 (650) 422-3624
info@zingbox.com

StartX
Stanford University
Part of StartX Startup Accelerator