Zingbox

HEALTHCARE
SOLUTION BRIEF

Comprehensive IoMT Governance, Now a Reality

For decades, healthcare providers have invested in the management and security of their IT resources, introducing technology, policy, and processes to track, safeguard, and optimize IT assets. However, many of the modern connected medical devices and IoT (Internet of Things) systems in healthcare organizations still remain unprotected and unmanaged. It's now time to apply the same rigor used to manage and secure IT to connected IoT systems and medical devices: the IoMT or Internet of Medical Things.

HEALTHCARE SECURITY CONCERNS

Most attacked industry since 2015

90% of hospitals are cyberthreat victims

75% of network traffic in a hospital is unmonitored

73% of hospitals do not have a security strategy for medical devices

17% of confirmed attacks originate from connected medical endpoints

It is estimated that 28 billion things will connect to the Internet by 2020 with little to no security, despite an increasing amount of sensitive data flowing through many of them. While the IT infrastructure is comprised of a standardized and limited number of operating systems and platforms, IoMT assets are often part of a heavily fragmented ecosystem of non-standardized, purpose-built devices. With such scale, diversity, and the typically limited system resources on IoT devices, existing security solutions simply don't work.

A new, reimagined approach to security is needed: an approach that can identify, secure and manage the IoMT devices while ensuring the lower total cost of ownership (TCO).

Through machine learning, artificial intelligence, and threat intelligence, Zingbox makes it possible to orchestrate the entire life cycle of the IoMT infrastructure.

Security

- Learn normal behaviors, report deviations, and allow only what's essential
- Assess risks and vulnerabilities
- Dynamically micro-segment assets to reduce threat exposure
- Meet security and compliance requirements (for example, HIPAA)

Management

- Provide ongoing device management with real-time monitoring, reporting, and reprovisioning
- Automate orchestration of the entire IoMT lifecycle
- Perform PHI leakage and application risk analysis

Optimization

- Improve capital planning due to improved device usage insight
- Improve patient experience and reduce wait times
- Minimize downtime through intelligently scheduled maintenance
- Link to enterprise applications (IT, OT and business)

ABOUT ZINGBOX

Proven healthcare expertise

Deployed in over 100 hospitals, protecting over 100,000 different types of IoMT devices

AI and machine learning

Leverages AI and ML to identify device personalities and assess behaviors

Real-world experience

Industry knowledge and know-how from 3 years of real-world deployments

Solution ecosystem

Industry-leading technology integrations, partnerships, and strategic alliances

ZINGBOX MILESTONES

2014

- Founded

2016

- First solution in a market-defining category

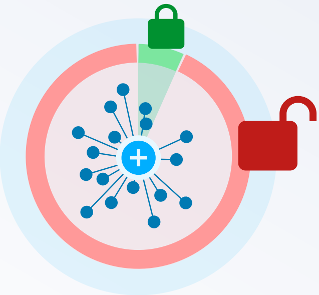
2017

- Japan Expansion
- Gartner Cool Vendor Award

2018

- Technology Alliances – VMware, Cisco, Fortinet, HP/Aruba, Gigamon

1.6+ PB of IoT data analyzed each day



95% of medical devices have **no endpoint security**

Security

As cybercriminals increasingly target healthcare service providers, the security of medical devices, the network, and vital assets like patient records, personnel files, and financial data is at greater risk than ever. To assess exactly what level of risk, it's necessary to learn the vulnerabilities of each device, the threats that target it, when it behaves normally and when it doesn't, and its access privileges on the network. Unfortunately, medical equipment does not support endpoint security applications, weakening its defenses. In addition, because medical equipment is sensitive to scanning, vulnerability scanners are often disabled, which creates security blind spots.

Zingbox Solution

Zingbox uses machine learning, artificial intelligence, and threat intelligence to identify and profile devices, analyze their behavior, and assess vulnerabilities and risks. Zingbox orchestrates the remediation of identified risks and threats, and enables context-aware microsegmentation by onboarding devices to appropriate network segments. This reduces the attack surface and enables compensating controls that permit only trusted behaviors. Through this approach to medical device security, Zingbox helps keep healthcare facilities up and running and patients safe and sound.

75% of network traffic in a hospital is **unmonitored**

Management

While many IoMT devices are connected to the network, most of them remain unmanaged. This is due to the large diversity of IoT devices and regulated environments that result in a lack of on-device agents for management. Providing centralized, automated, and ongoing management for IoMT devices from onboarding to decommissioning has become a growing challenge for healthcare organizations.

Zingbox Solution

IoT Guardian uses artificial intelligence to automatically identify devices and learn each device's unique personalities, enabling dynamic asset management. It simplifies the monitoring, reporting, upgrading, and reprovisioning of connected devices through the automated orchestration of the device life cycle. This allows healthcare organizations to not only discover but control and manage their connected IoMT devices in real time.

<30% **peak utilization** for infusion pumps

Optimization

Biomed teams often find themselves over budget while medical devices remain underutilized and maintenance costs soar. Monitoring clinical assets can help optimize utilization and reduce the total cost of ownership. However, to collect this data and monitor it manually would be such a tedious and time-consuming enterprise that it is rarely if ever done.

Zingbox Solution

IoT Guardian constantly monitors device traffic and, with its deep knowledge of device behavior, tracks the degree to which every IoT and IoMT device on the network is used for better capital planning. Furthermore, with this data, a maintenance schedule can be tailored to the actual utilization of each device rather than be based on a length of time.

For more information, visit zingbox.com