nuvolo Zingbox

Solution Brief

Mitigate IoT Cyber Security Threats Using Zingbox and Nuvolo

THE **CHALLENGE**

Today's healthcare systems face a stark and increasingly pervasive threat stemming from the propagation of connected medical devices. In addition to more IoT enabled devices, both the quantity and severity of cyber security threats is expanding at a furious pace. Exposure and liability for the healthcare system includes brand risk, disruption to patient care, patient safety, the threat of ransom ware demands and loss, and black-market sale of patient data. To better manage these threats, new technology and modern processes must support a new level of cooperation between clinical engineering, IT, and security operations.

The first step toward an effective security solution for connected medical devices is to base it on an accurate and trusted device inventory. A trusted medical device inventory with standardized contextual data had been elusive for modern health care systems. This challenge is second only to maintaining the validity of the inventory and related data over time. The absence of modern tooling and processes forces the health system to rely on manual physical inventories and a cyclical data refresh. The inherent inefficiencies and expense of these processes are compounded by the absence of a single, trusted system of record for medical device inventory. Manual device identification and disparate systems of record pose a material risk for the healthcare system.

The absence of a trusted, accurate and real-time device inventory can greatly limit the effectiveness of even the most advanced security solution. Standardized contextual medical device data including device location, owner, escalation contact, risk profile, network data, make, model, description, and other essential information are necessities for all modern healthcare providers. These contexts facilitate both the correlation of affected devices across the fleet, and appropriate remediation processes for cyber security threats. Health system-wide risk mitigation requires discovering and understanding affected devices and remediating threats quickly and efficiently. The impediments to this process include legacy discovery and security operations technology, disparate data, multiple disconnected systems and non-standard taxonomy and nomenclature within the existing systems of record. These issues create an enormous and unsustainable risk for the health care system.

Moving beyond just data protection to full service protection for business continuity means obtaining actionable data on threats, understanding risk,and swiftly executing on remediation. The goal is improved security intelligence for reduced healthcare system exposure.

nuvolo Zingbox

Solution Brief

SOLUTION **Features**

- Automatically discover, identify and classify devices
- Correlate identified threat details
- Continuous non-intrusive monitoring
- Contextualize data and enhance value
- Remediate threats quickly and efficiently
- Real-time inventory of connected medical devices
- Closed-loop remediation from detection of threats to trouble ticketing

THE **SOLUTION**

Zingbox and Nuvolo meet the cyber security demands of a modern health care system by providing a compelling medical device cyber security management capability.

Combining AI-powered device discovery and threat detection capabilities together with an enterprise security response platform, the integrated solution delivers rapid and efficient cyber security threat mitigation.

The integrated platform brings together deep knowledge and understanding of trusted device behavior with rich contextual data to inform security operations on the precise nature of a vulnerability or event. The rich device contextual data, cyber work flow, and orchestration capability then informs the remediation process, determines prioritization, and manages work. The primary goal is to address the known vulnerability. Once contained, the integrated platform leverages its native matching algorithms to identify and match additional at-risk IoT devices within the inventory.

All cyber security management integration between Zingbox and Nuvolo are securely recorded with date and time stamps. The audit trail can be used for post incident review, audit, reporting, and service management worker training.

ABOUT **ZINGBOX**

Enabling the Internet of Trusted Things, Zingbox provides hospitals, companies and manufacturing facilities with Internet of Things (IoT) security software that helps ensure service delivery. Zingbox's new approach is based on deep learning and enforcement of trusted behavior. Founded by Silicon Valley veterans with expertise in cyber security, IoT, deep learning and networking. Privately held and founded in 2014, Zingbox is headquartered in Mountain View, CA.

For more information, visit: www.zingbox.com

ABOUT **NUVOLO**

Nuvolo is revolutionizing medical device cyber security by innovating on Service Now, the world's leading enterprise cloud platform. The company's vision is to be the global leader in cyber security for enterprise operating technology, powered by a culture of innovation and a relentless commitment to customer service. Privately held and founded in 2013, Nuvolo is headquartered in Paramus, NJ with offices throughout the U.S. and internationally in London and Pune, India.

For more information, visit: www.nuvolo.com