

SMART HEALTHCARE SOLUTION:

Securing and Managing the Internet of Medical Things

KEY BENEFITS

Predictive and Preventative Security

- Eliminate tampering of medical equipment and PHI by detecting Zero-Day and advanced persistent threats (APTs)
- Provide real time Over The Air security updates to all IoT devices and equipment connected by supporting gateways (even if they are remote and in unmanned locations)

Improved Inventory Management and Tracking

- Reduce inventory loss due to theft/misplacement (expensive surgical kits, wheelchairs, trolleys etc.) by enabling real time asset tracking
- Enable clinical engineers to plan better for outages and spare devices by getting real-time insight into inventory and eliminate the need for manual tracking with spreadsheets and static databases
- Have complete visibility and control of all connected medical devices within CMMS solutions

Optimized Operations

- Enable clinical engineers to adopt Alternate Equipment Maintenance (AEM) programs by tracking device utilization metrics in real time and not time-based intervals that limit effective device deployment
- Improve future device selection decisions by gaining detailed device insight to assess device risk and vulnerabilities



Zingbox and VMware Pulse's joint solution helps healthcare organizations build a secure and robust IoT infrastructure foundation that reduces the time to value of their IoT use cases so that companies can focus on what matters the most - creating an efficient and responsive healthcare system to deliver excellent patient care.

Adoption of connected devices like smart equipment, sensors and medical wearables is revolutionizing all aspects of healthcare, be it improving patient care and treatment adherence, optimizing staff and hospital operations, or enabling predictive medicine. However, the addition of these numerous devices to traditional networks is also increasing the surface area of threats. Correct precautions need to be taken to ensure device safety to avoid unauthorized access of medical devices and PHI (Personal Health Information).

KEY BENEFITS

Maintain Business Continuity

- Enjoy complete flexibility in defining and tracking which thing or gateway is updated, when and where, and by whom
- Get uninterrupted availability of connected medical devices by reducing the need for manual room-to-room device audits, and time-based device maintenance plans

Meets the Needs of Both OT and IT Departments

- IT approved solution that meets the needs of your operational technology (clinical engineering department)
- Choose from a wide variety of devices based on functionality and not necessarily by the limitation of what devices can be managed and secured, since VMware and Zingbox support device heterogeneity

LEARN MORE

<https://www.vmware.com/solutions/iot.html>

<https://www.zingbox.com/>

Blog: <https://blogs.vmware.com/pulseiot/>

Twitter: @vmwareiot

LinkedIn: @vmware-iot

Some of the challenges healthcare companies face while embracing IoT are:

1. Safe onboarding of IoT devices onto existing systems and networks
2. Managing heterogeneous devices with different operating systems, makes, and models
3. Maintaining ongoing device security with minimal process interruption

Zingbox and VMware: Smart Healthcare

Zingbox and VMware are teaming up to solve these issues and provide a solution that integrates Zingbox IoT Guardian, Artificial Intelligence (AI)-driven personality-based IoT security solution with VMware Pulse IoT Center, an IoT device management and monitoring solution. Zingbox introduces the element of trust between IoT devices by discerning each device's unique personality and enforcing acceptable behavior. VMware Pulse IoT Center provides vendor-neutral open source SDK to enforce IoT rules.

About Zingbox

Enabling the Internet of Trusted Things, Zingbox is the industry's first and only IoT security solution provider to leverage the individual personalities of IoT devices to provide accurate visibility and protection of an organization's IoT assets. IoT Guardian, Zingbox's SaaS-based security solution, leverages machine learning to discover IoT devices, assess risk, baseline normal behavior, detect anomalous activities, and provide real-time remediation across an organization's entire IoT footprint.

About VMware Pulse

VMware Pulse IoT Center is a secure, enterprise grade, IoT device management and monitoring solution that helps both Information Technology (IT) and Operational Technology (OT) organizations to onboard, manage, monitor and secure their IoT use cases from the edge to the cloud.

