Is Cyber Risk in the Nature of IoT ?

Jun Du

Head of Security Research and Analytics

Agenda

- The “Connected” Challenge
- AI is Driving the Technology Advancements
- Insights from Real World Data

About Zingbox

AI-based security for the Internet of Things (IoT)

Founded in 2014, based in Silicon Valley

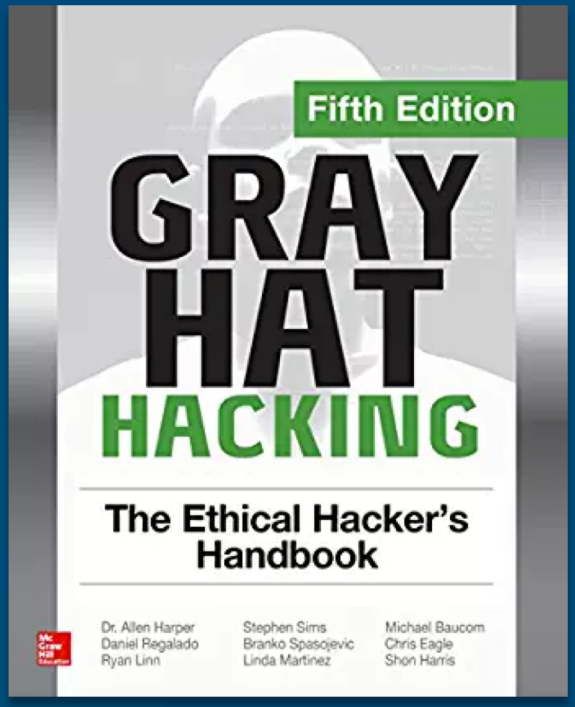
StartX Stanford University

Incubated out of Stanford

Gartner Cool Vendor 2017

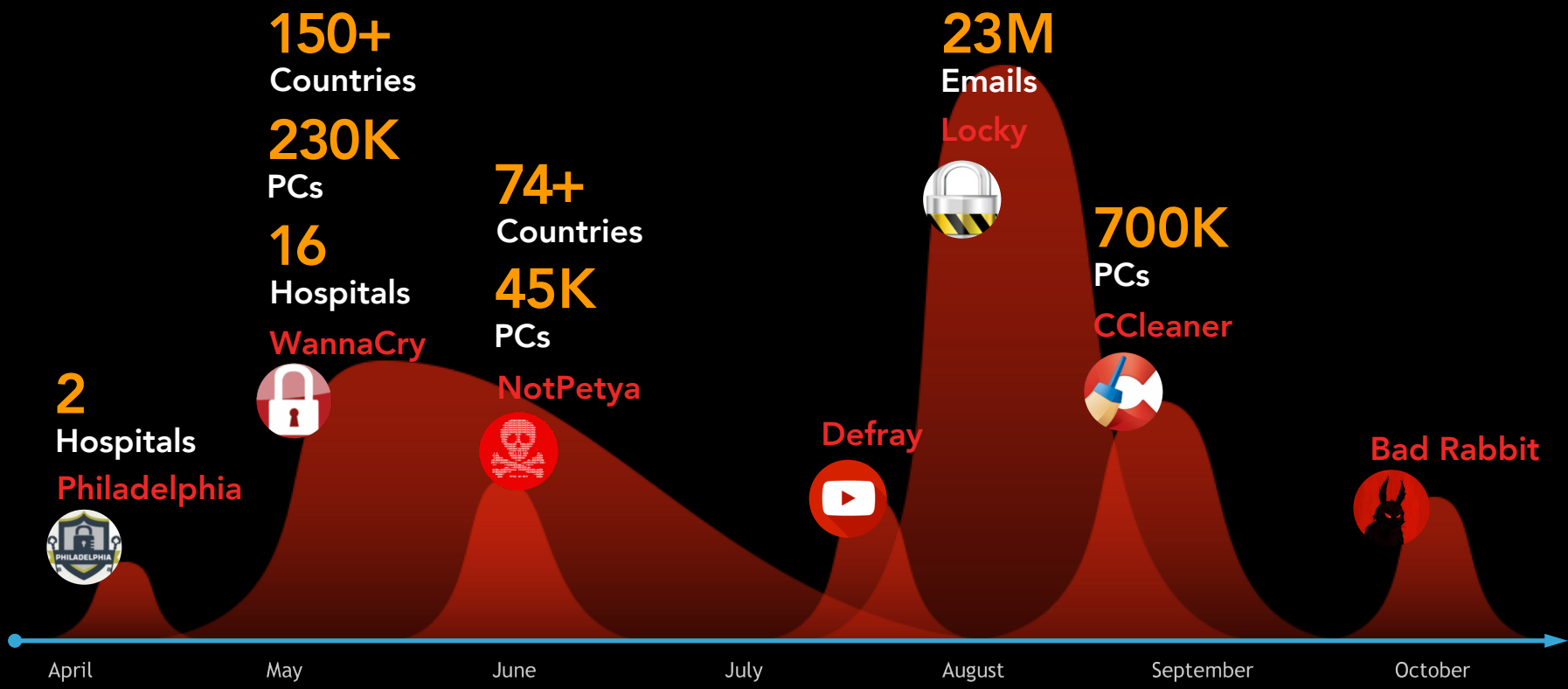
Gartner Cool Vendor in IoT Security

Large deployments in the real world


Fifth Edition
GRAY HAT HACKING
The Ethical Hacker's Handbook
Dr. Allen Harper
Daniel Regalado
Ryan Linn
Stephen Sims
Branko Spasojevic
Linda Martinez
Michael Baucom
Chris Eagle
Shon Harris

Challenges

Hacking Healthcare 2017



Zingbox

More Devices are Connected

Improved efficiency

Reduced cost

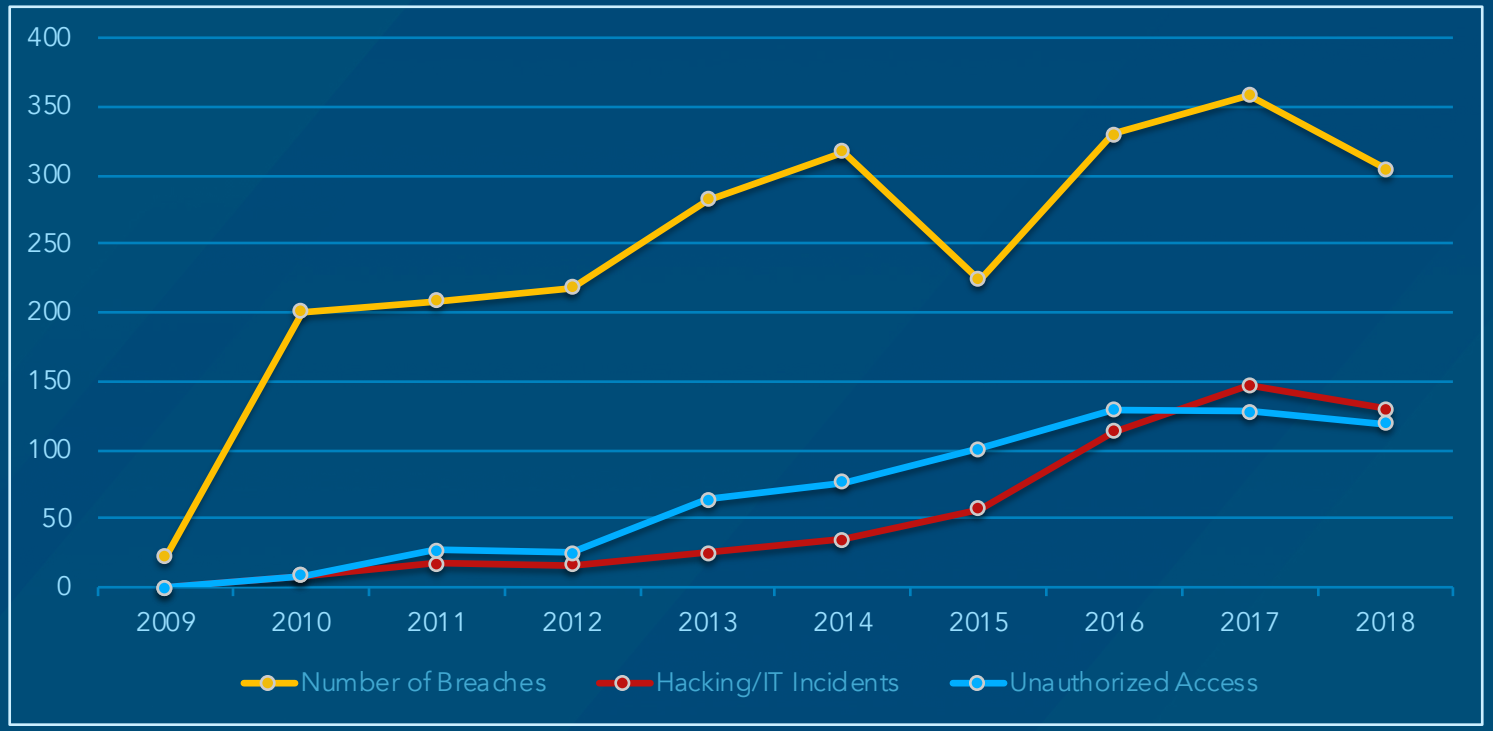
Increased revenue

Information breach

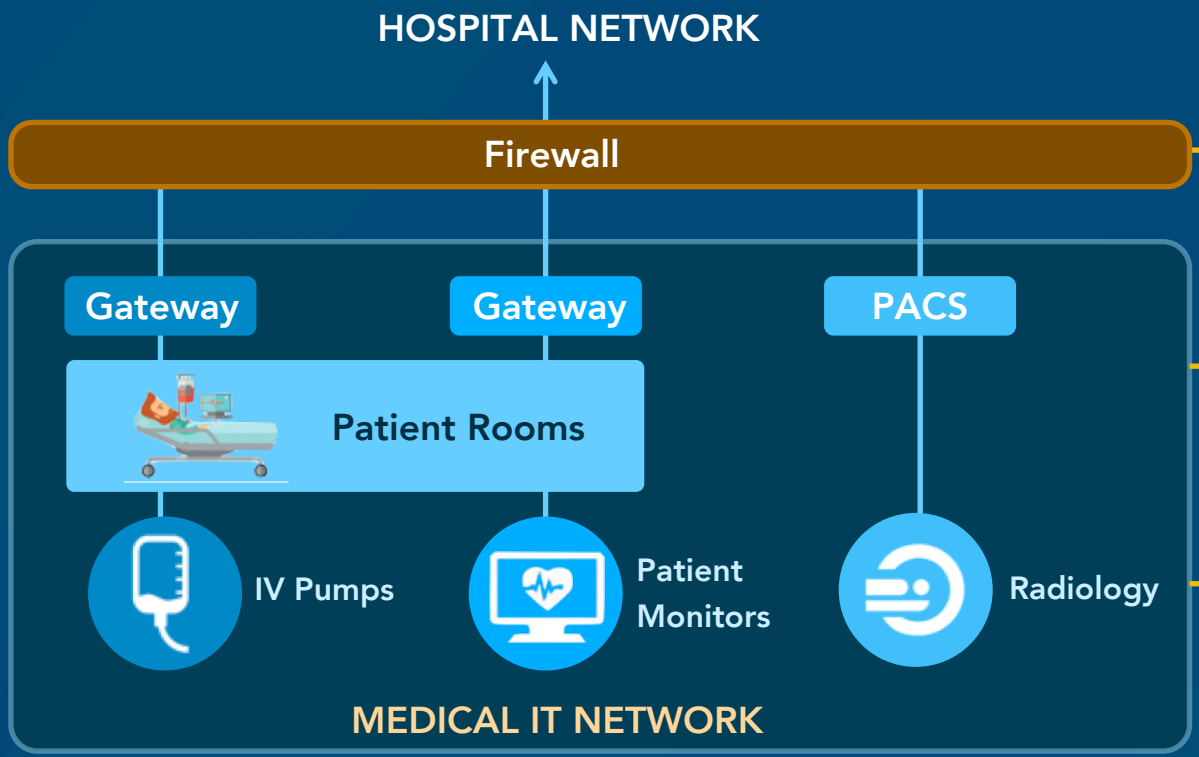
Operation interruption

Patient safety

Hacking Healthcare



Connected Without Protection



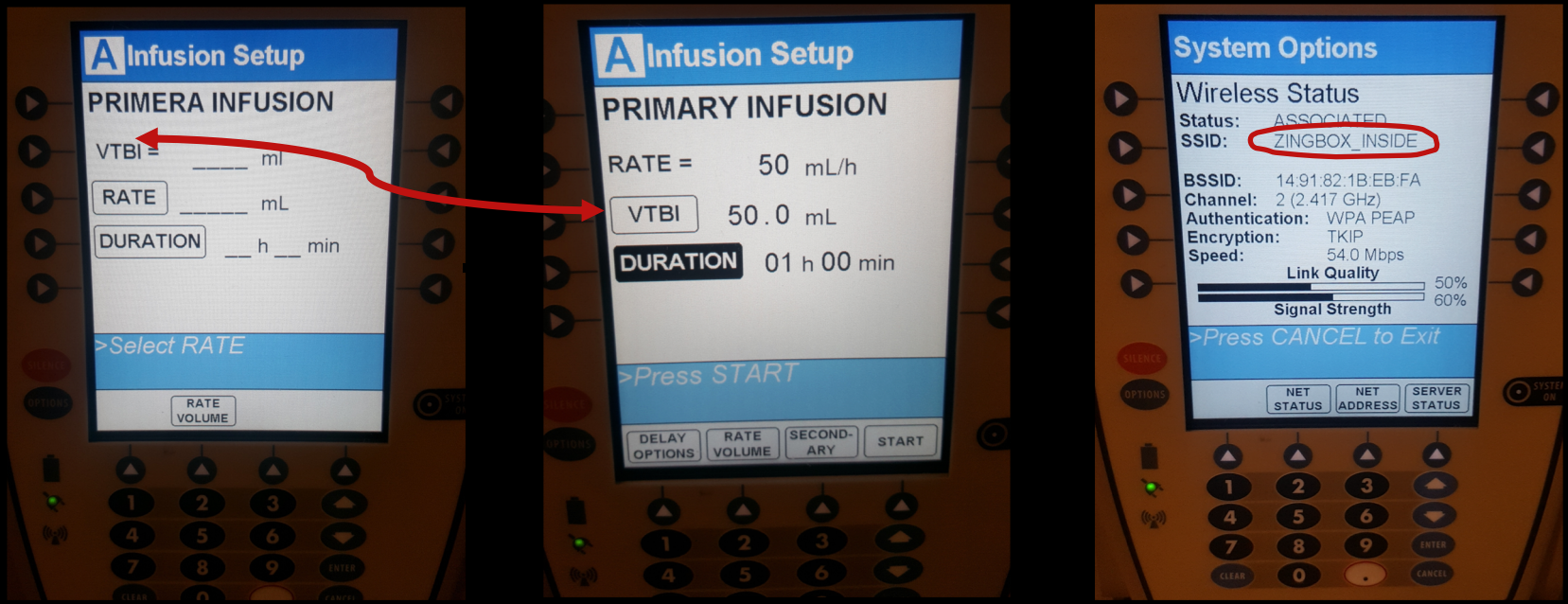
The single line of defense

Unmonitored network

Lack of endpoint visibility & security

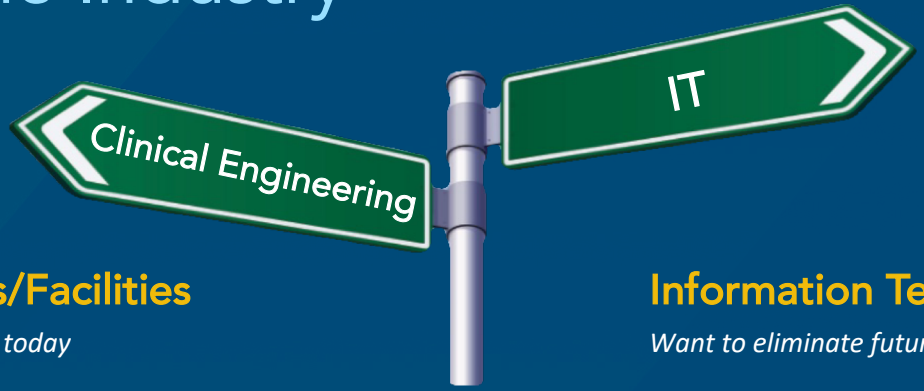
The Immense Attack Surface

IV Pump Over Dosage, WIFI Take-over



Zingbox

A Shift in the Industry



Operations/Facilities

Own the problem today

GOALS

Business continuity & patient safety
Operations & compliance
Equipment maintenance & security

LIMITATIONS

Lack security tools
IT solutions don't work

Information Technology

Want to eliminate future risks

GOALS

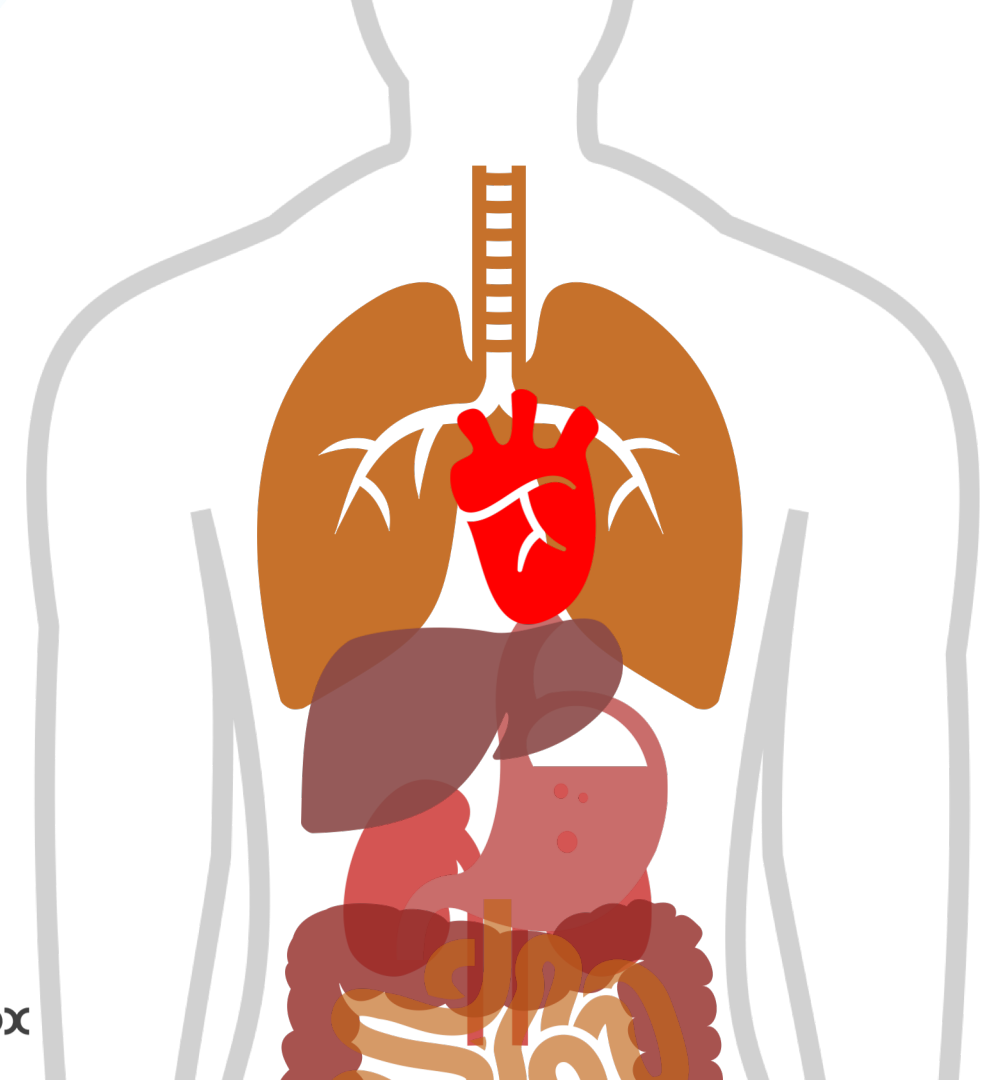
Cybersecurity across the org.
Risk assessment
Data protection

LIMITATIONS

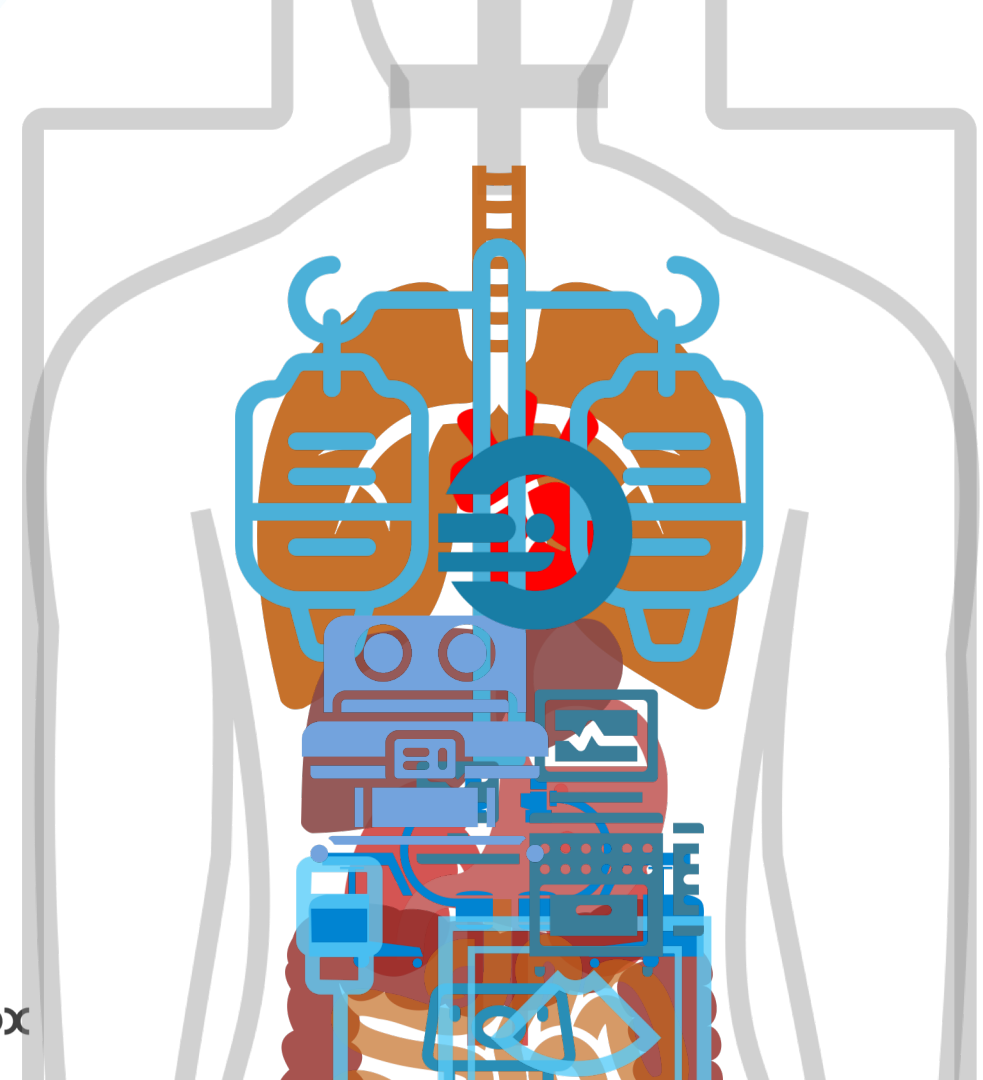
Can't touch medical assets, no agents
Highly regulated industry
No visibility into clinical networks

Cyber Risk in the Nature of IoT

- Large quantity
- Large variety
- Long life cycle
- Large surface
- Lack of protection

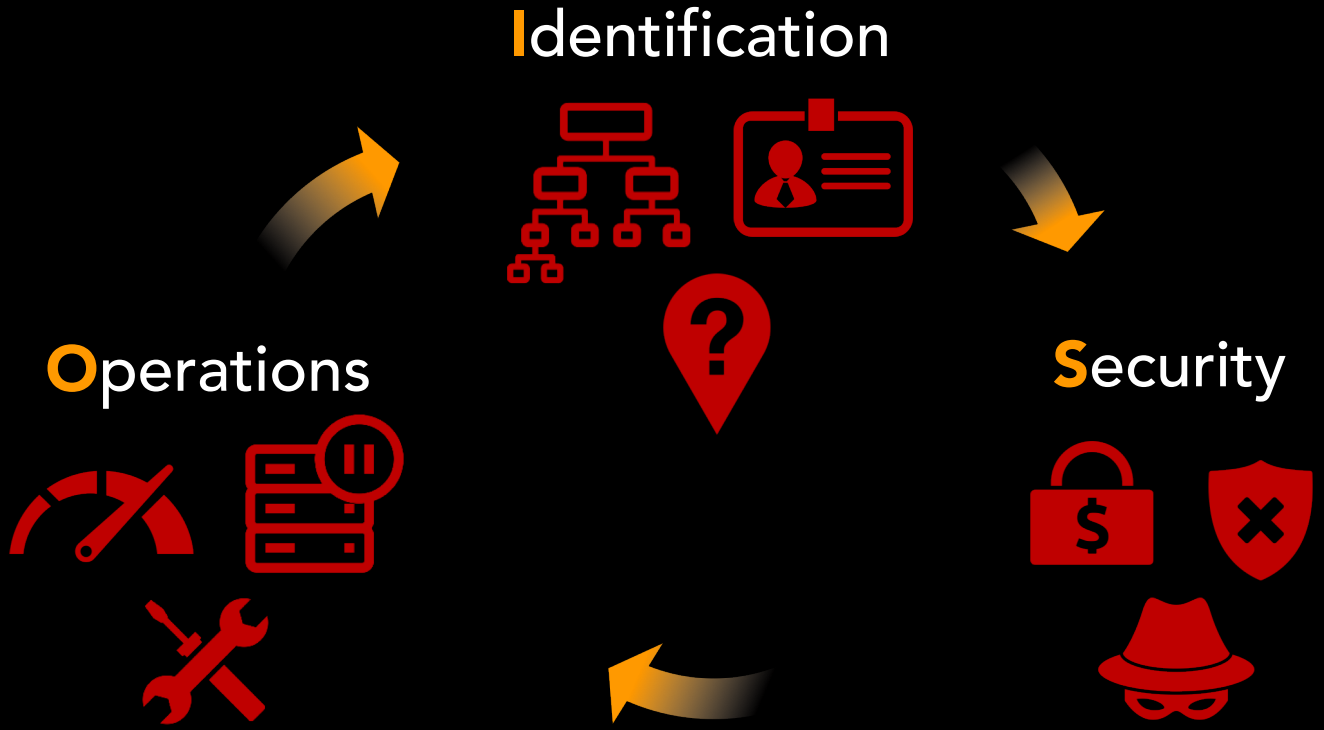


The Internet of Things (IoT)



The Internet of Things (IoT)

The “Connected” Challenge: ISO



Zingbox

Which device has this mac address?

How many medical devices are active on my network?

Which devices contain PHI?

How to prevent the next WannaCry?

Are medical devices safe when malware is found on IT servers?

How to contain an infected device without impacting patient care?

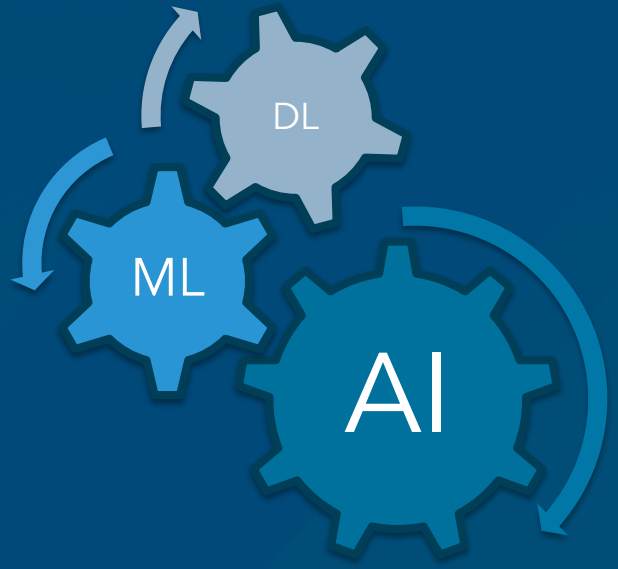
How to maximize device utilization?

How many additional IV pump do I need?

How to leverage on the existing IT security tools?

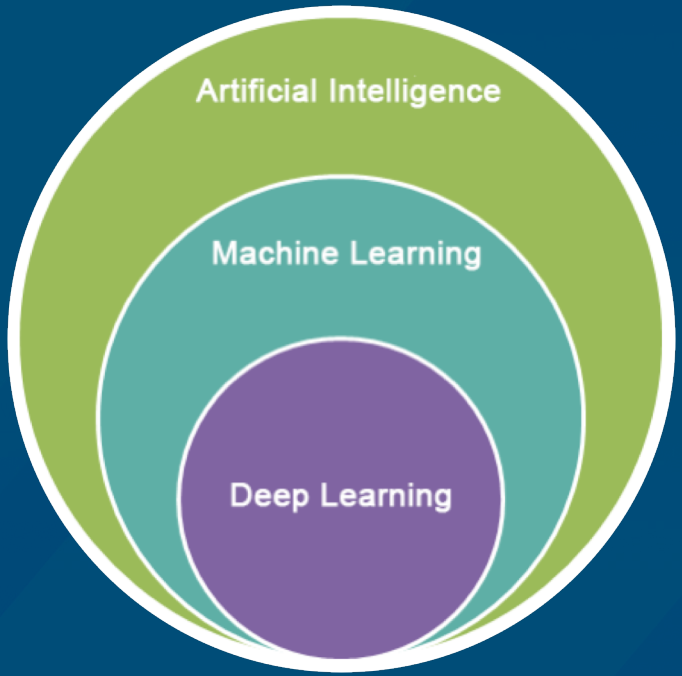
Possible Solutions

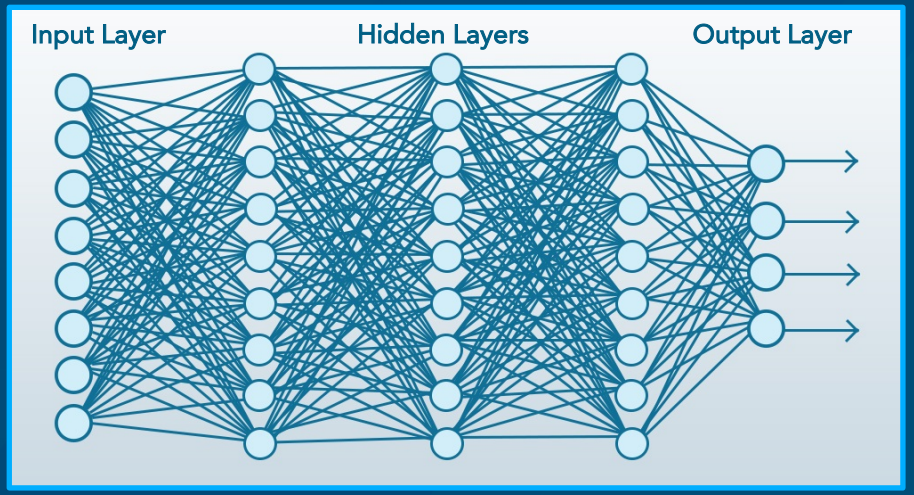
- Agentless
- Device Identification
- Operational Status
- Edge + Cloud
- Micro-segmentation
- IPv6 Security
- Scalability for data
- Easy to use
- Automatic



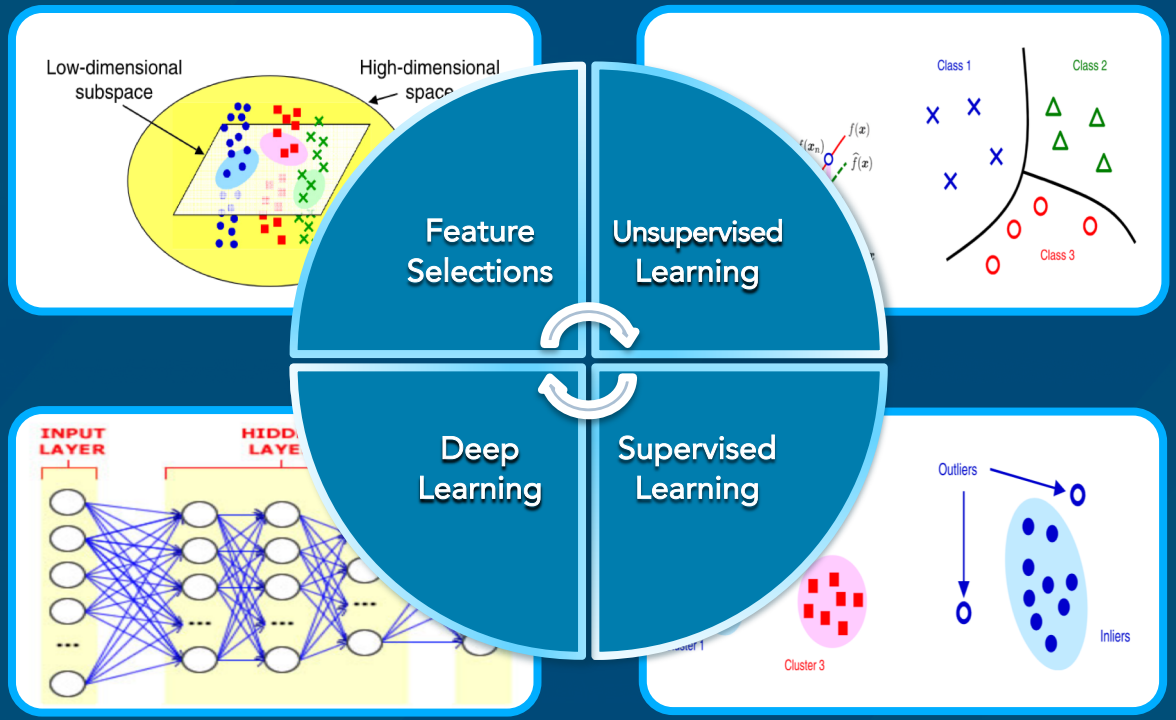
AI: Artificial Intelligence

From Automation to Deep Learning

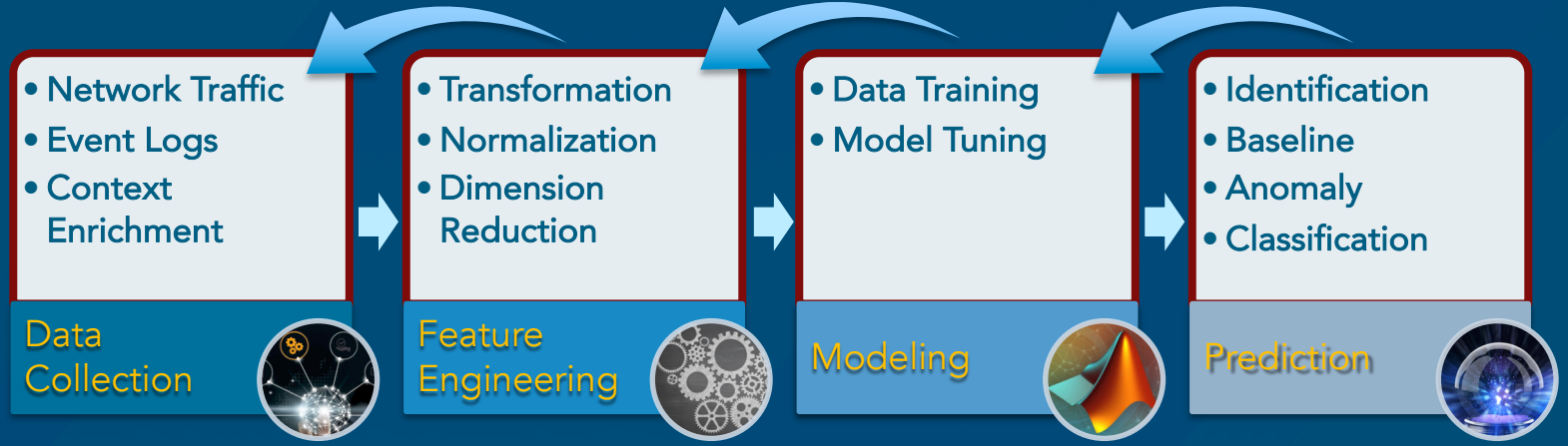




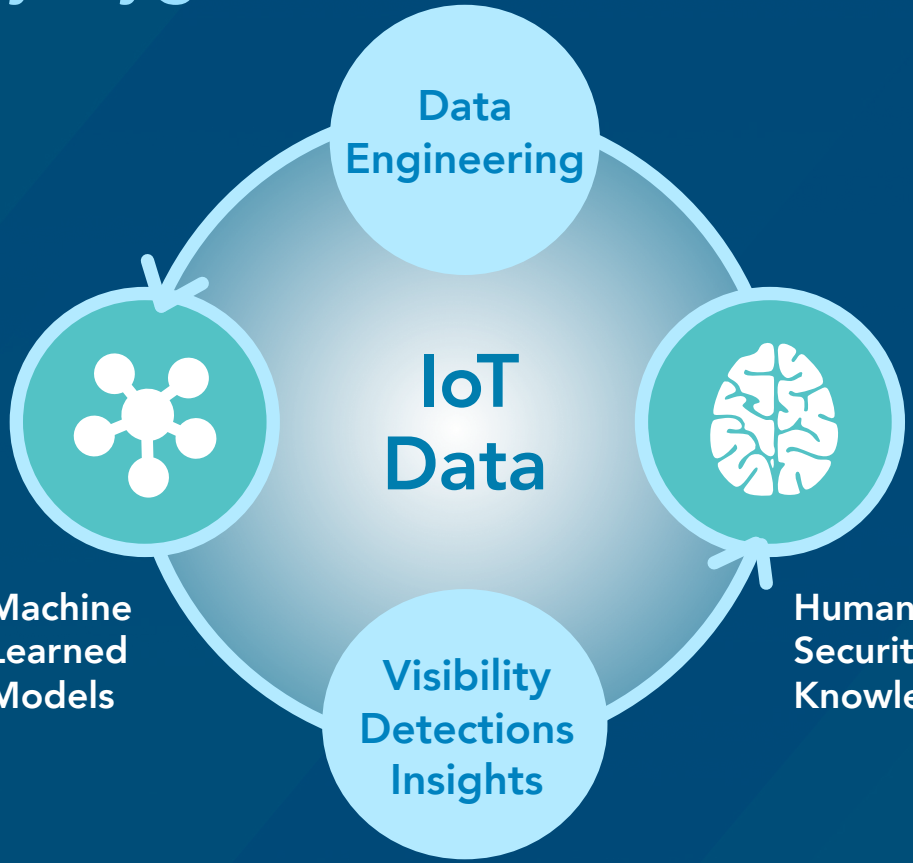
Elements of AI in IoT Security



Workflow of AI in IoT Security



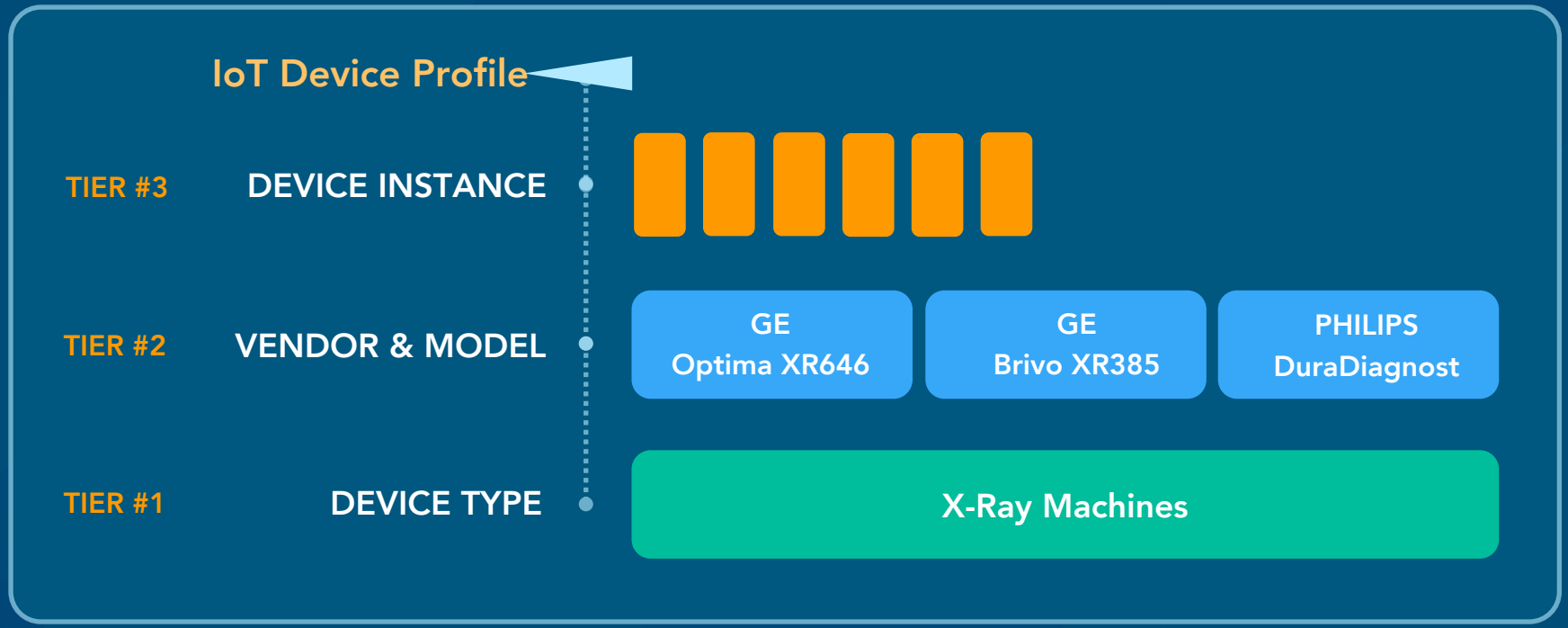
The Security Hygiene for Medical Devices – AI



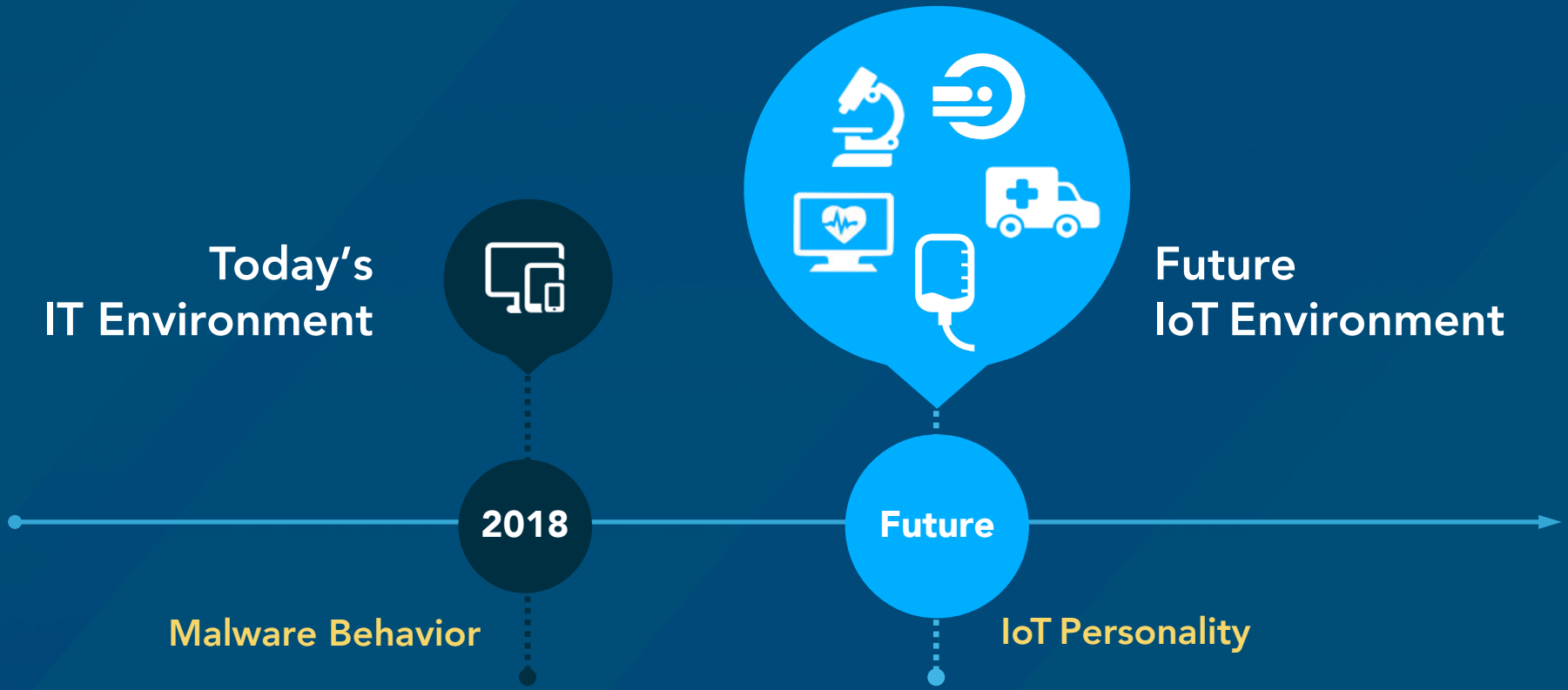
- Supervised Classifications
- Unsupervised Clustering
- Neural Networks

- Attack Scenarios
- What Looks Risky?
- What Breaks Policies?

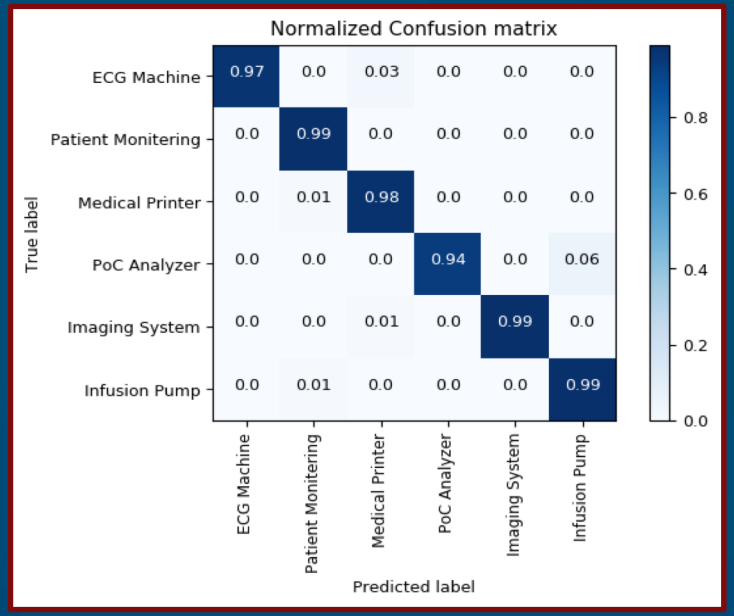
Medical Devices – Personality and Context

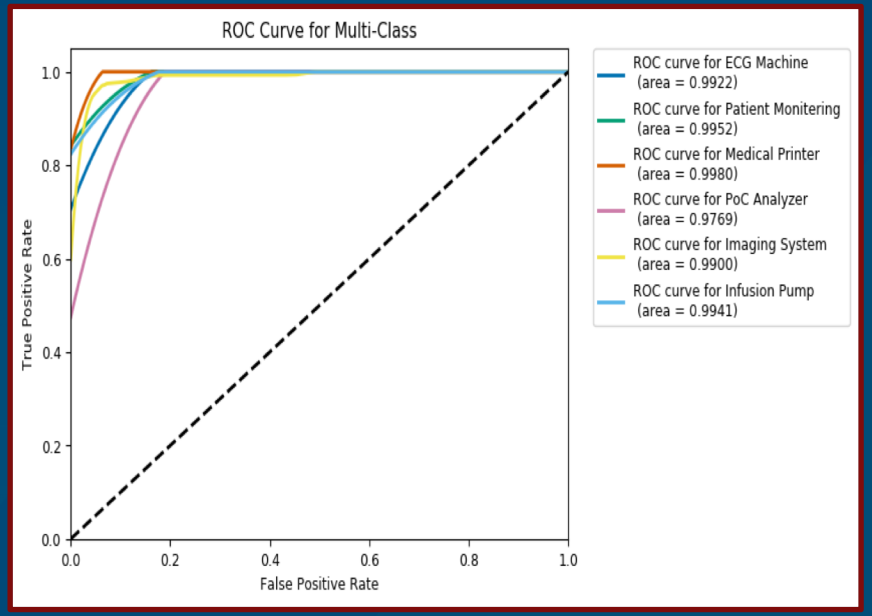


Entity Behavior Analytics

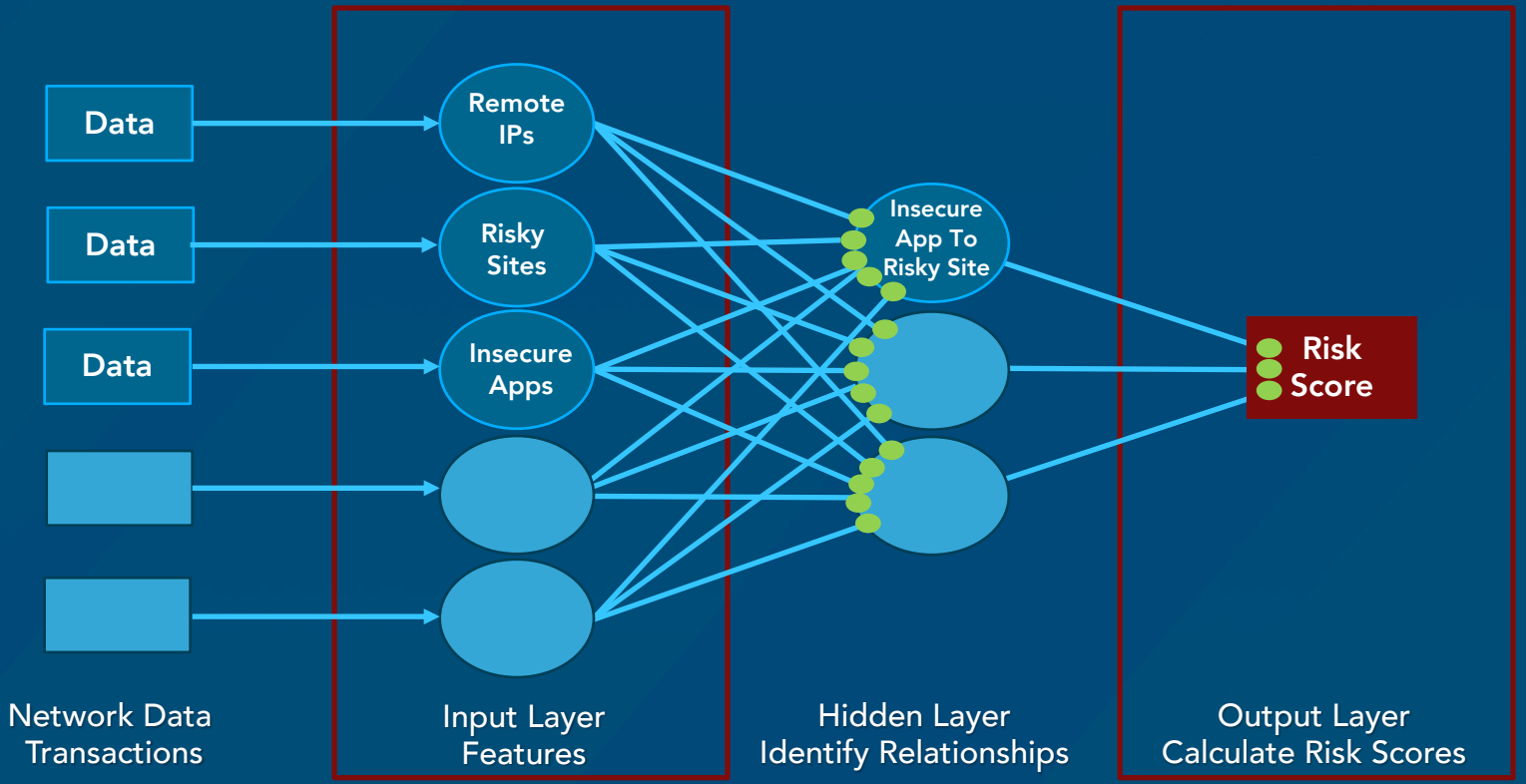


Medical Device Identification





Behavioral Risk Prediction



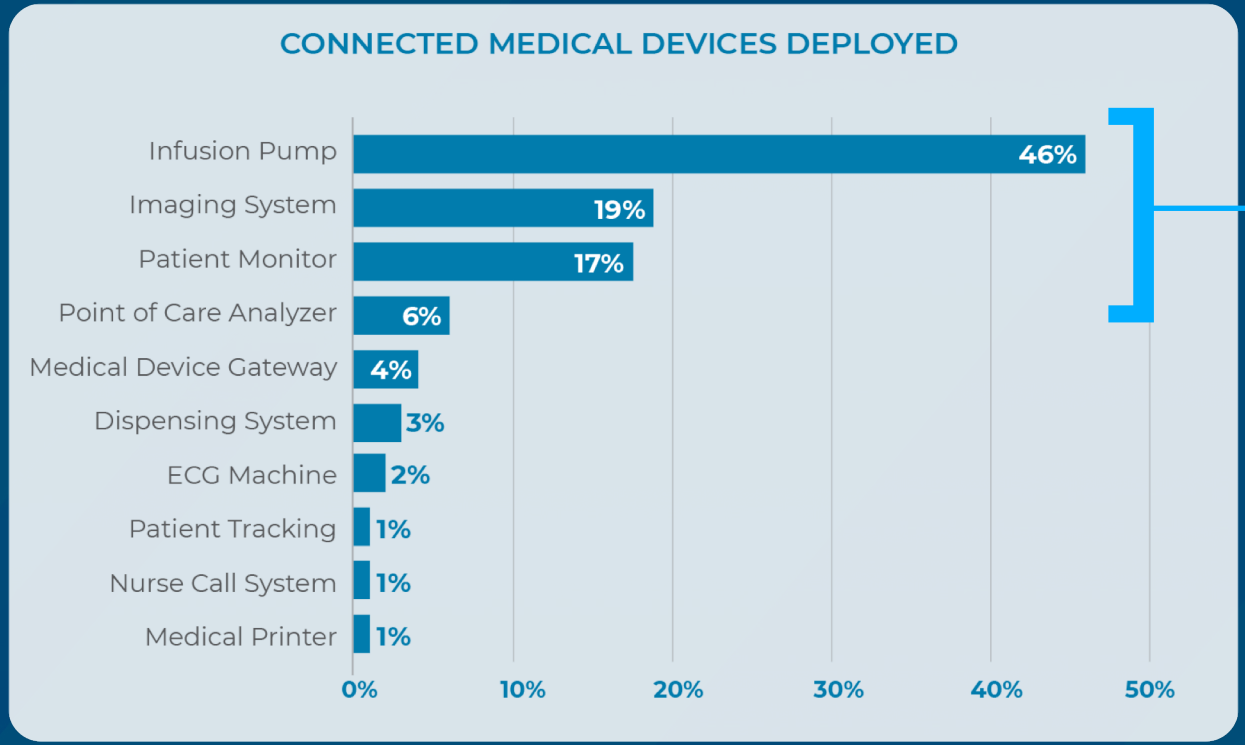
Zingbox

Data

Questions to Address

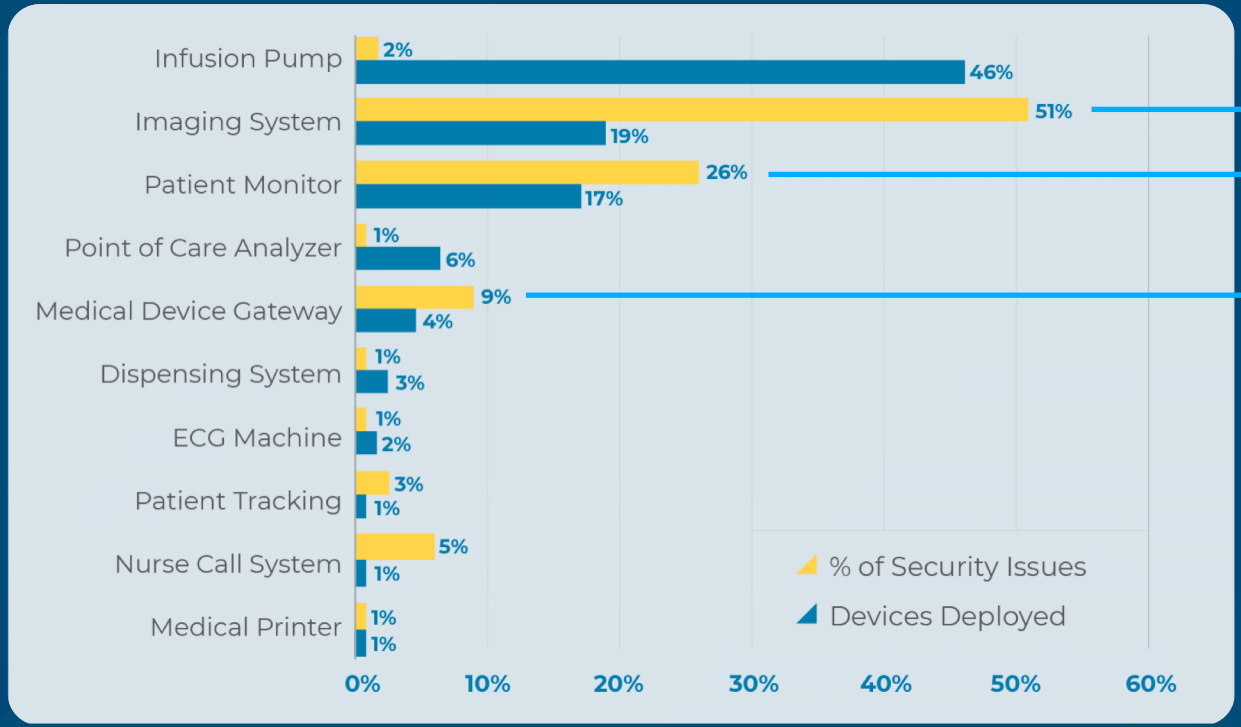
- What are the devices and their distributions?
- What devices are most vulnerable?
- What are the vulnerabilities?

What are the Devices ?



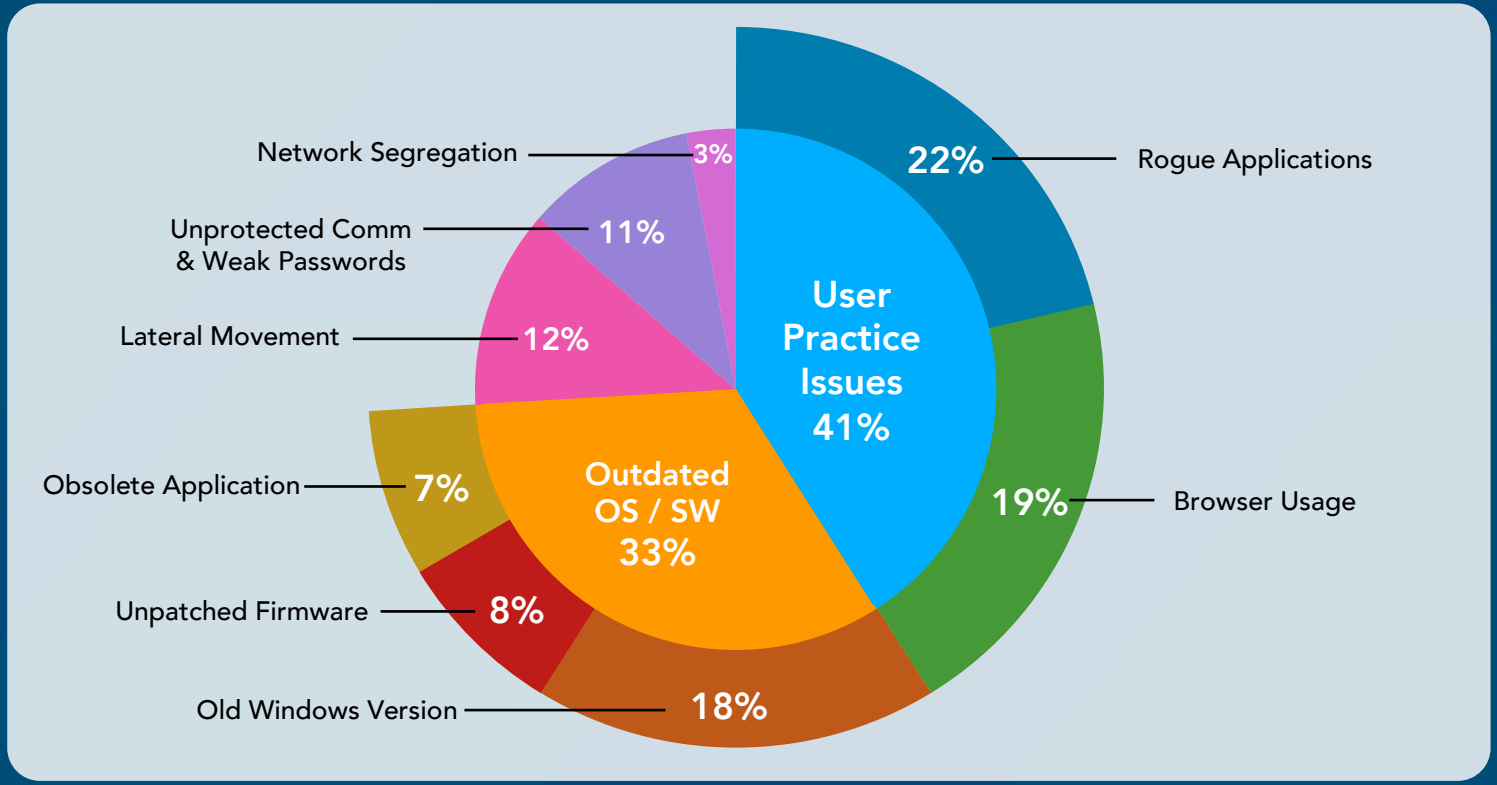
Three types make up **82%**

Most Vulnerable Devices

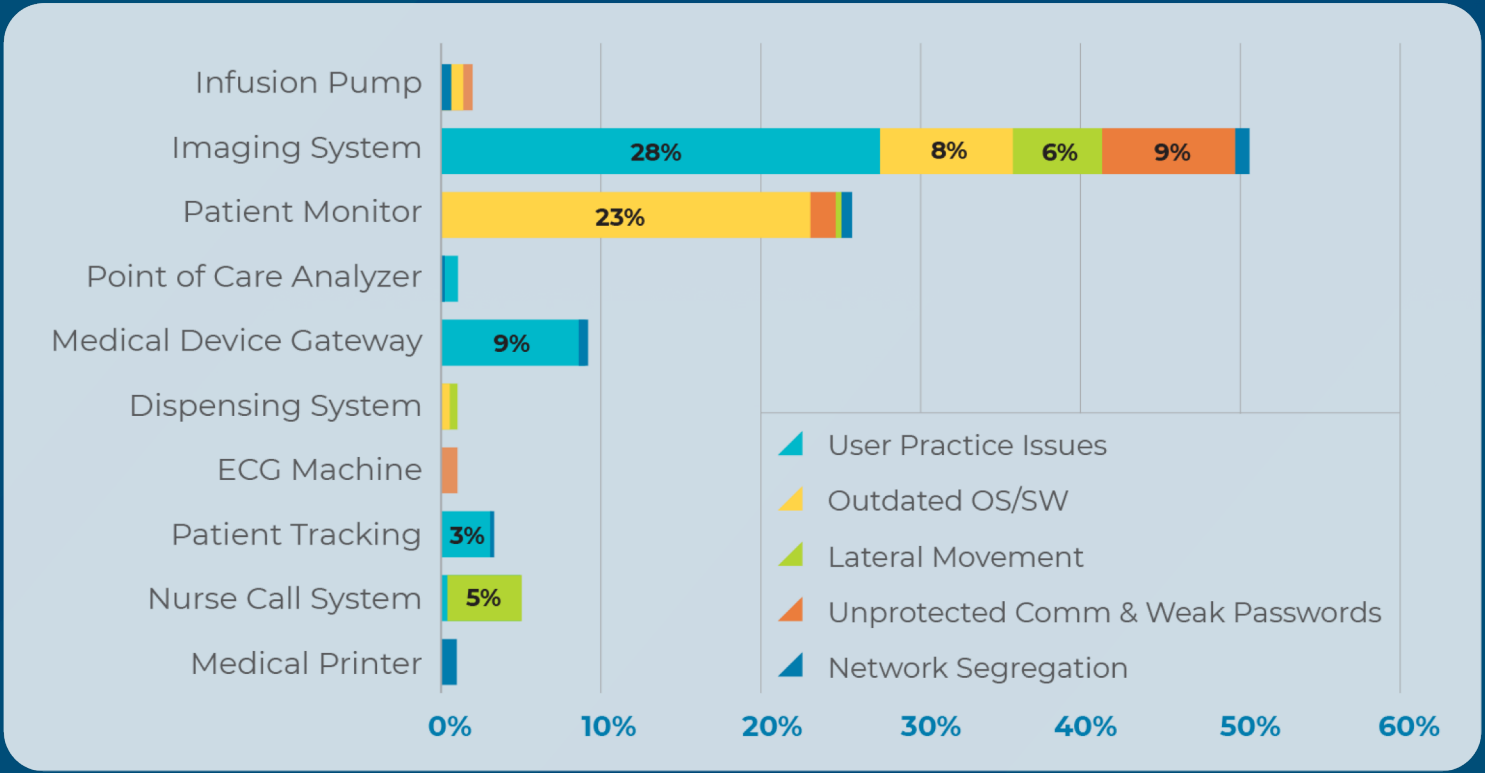


Three device types account for **86%** of security issues.

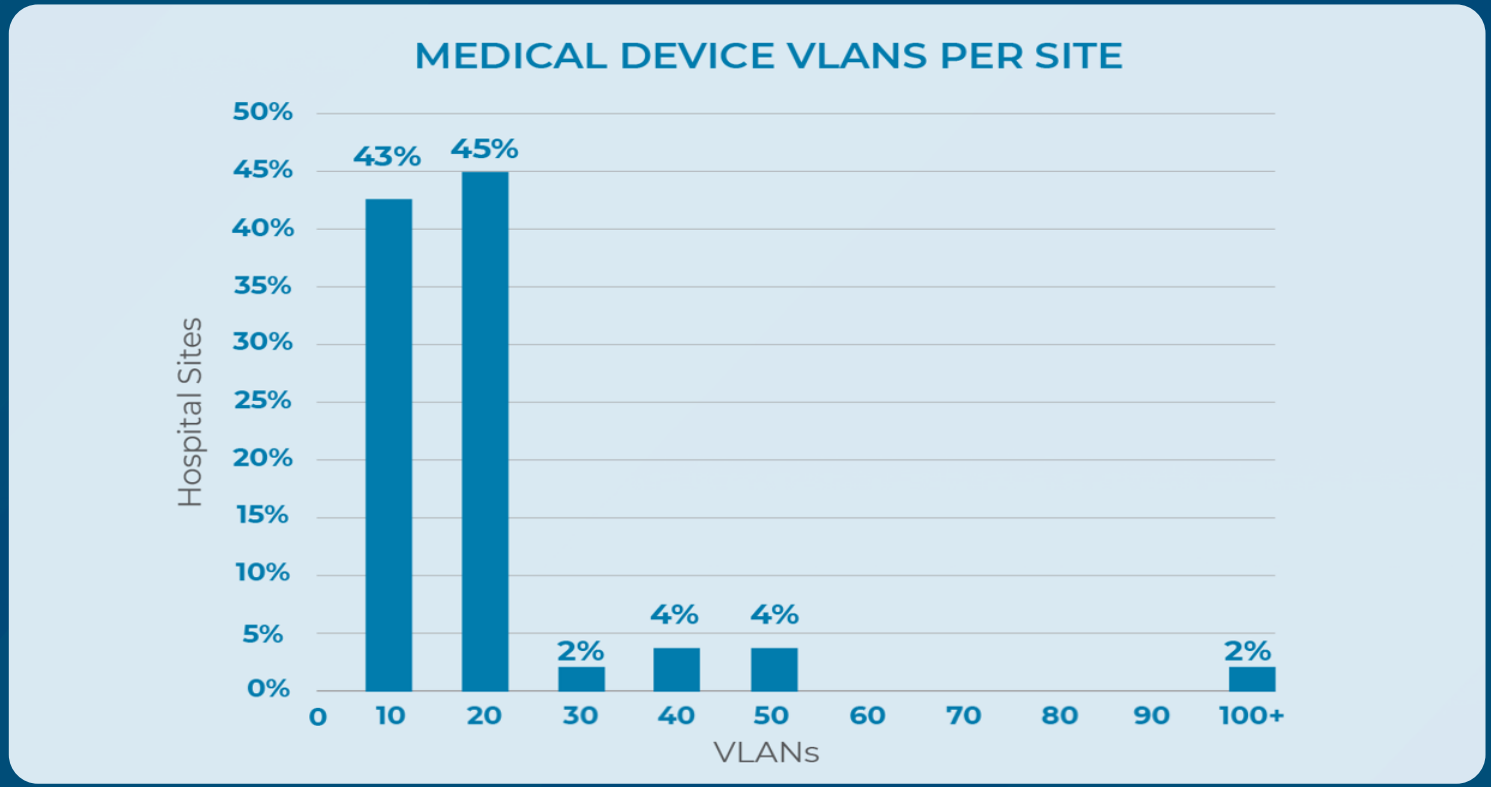
Types of Security Issues



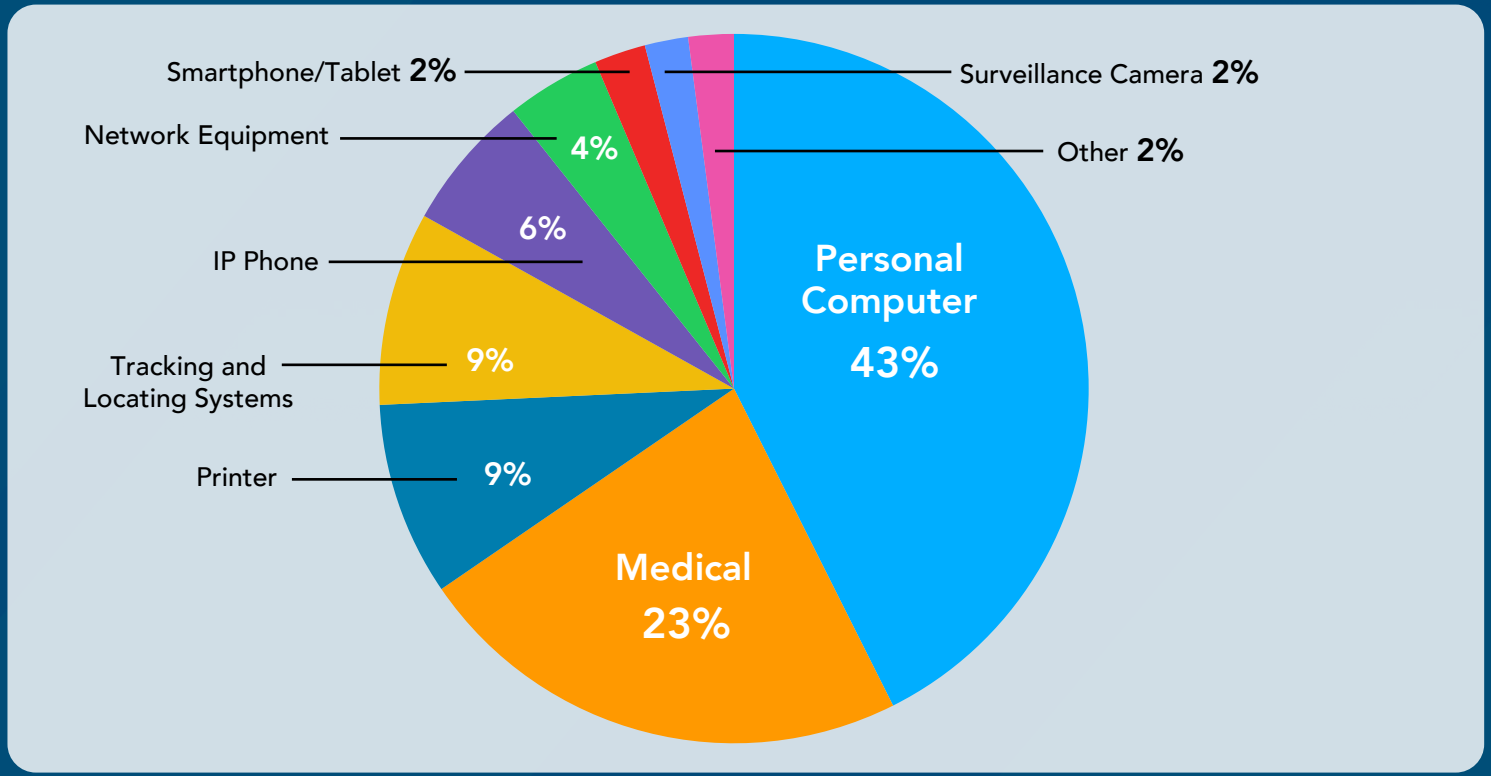
Security Issues by Device Type



Use of Micro-Segmentation



Today's Medical VLAN

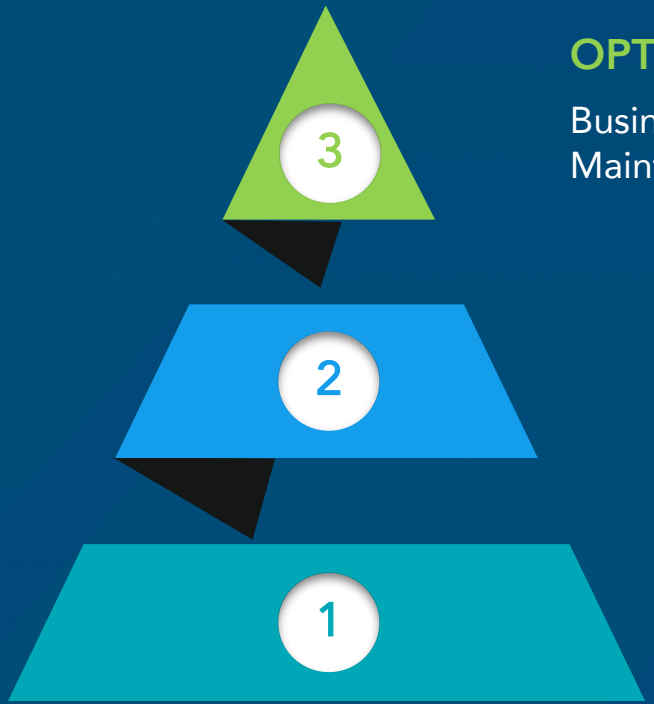


Download the Report

Full threat report is at:

http://www.zingbox.com

Complete IoMT Governance



OPTIMIZE

Business Efficiency , Capital Planning,
Maintenance Cost Reduction

PROTECT

Risk Management, Improved Security Posture,
Threat Containment, Regulatory Compliance

MANAGE

Identify & Classify Assets, Context Aware Micro-segmentation, Identity-based Policy Enforcement

Zingbox

Securing Devices, Saving Lives!

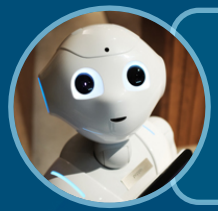
Challenges: **ISO**

Identification

Security

Operations

Solutions:



AI: automatic, continuous, proactive

Collaboration

More investment into securing medical devices

Enabling the Internet of *Trusted* Things

Jun Du

Jun.Du@zingbox.com