Identify the **Biggest Security Issues** Plaguing Connected Medical Devices

Protect Your Network with Unprecedented Insight

Medical devices and other Internet of Things (IoT) devices require a new approach to security. The lack of insight into the security issues plaguing these devices however, have left many healthcare providers paralyzed.

Zingbox IoT Guardian analyzed the behaviors of tens of thousands of medical devices at 50 hospitals to reveal the most common cybersecurity issues for connected medical devices. The results will surprise you.

3%

Network Segregation

Are the patient monitors in the same network as your PC?

11%

Weak Communication & Passwords

When is the last time you changed your password on an IV pump?

12%

Lateral Infection

Can imaging systems infect patient monitors? Of course they can!

41%

User Practice Issues

- Listening to your favorite tunes on an image viewer?
- Checking your personal email on a DICOM workstation?
- Downloading applications on a PACS Server?

It happens more often than you think. The biggest security issues for connected medical devices are due to user practice issues.

33%

Outdated OS/SW

Does the logo of a forgotten Window OS bring you back memories? Unpatched firmware and obsolete applications make up 8% and 7% of all security issues. Legacy Windows OS however, is the cause of security issues for 18% of all medical devices.

Zingbox

Arm yourself with the latest insights into the security issues plaguing connected medical devices. To learn how, visit zingbox.com/healthcare.