What Connected Medical Devices **pose the most risk?**

Prioritize your security efforts on devices that need it the most

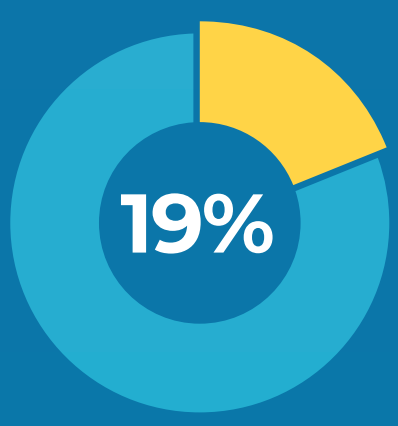
Identifying the type of connected medical devices that are causing the most security issues is the first step to formulating an effective management and security strategy.

Zingbox IoT Guardian analyzed behaviors of tens of thousands of devices to identify which devices exhibit the most security issues. Study reveals not all devices are built the same.

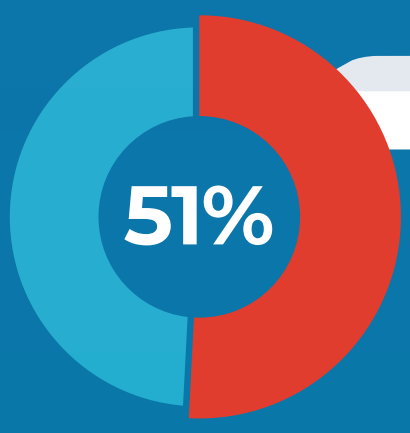
Imaging Systems

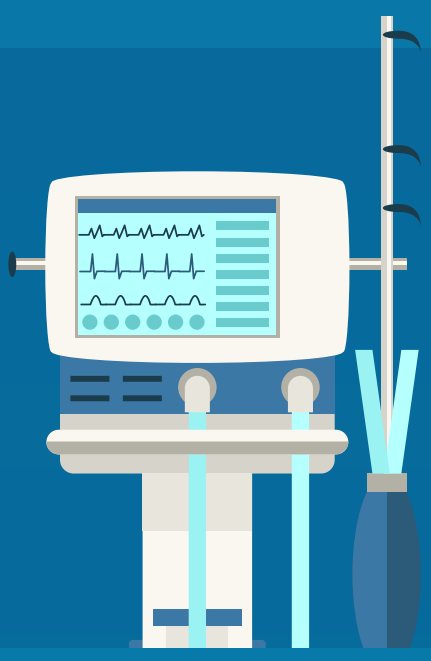
Web surfing on image viewers, checking social media feeds on DICOM workstations, and downloading your favorite app on PACS servers happen more often than you think. No wonder Imaging Systems account for more than half of all security issues in connected medical devices.

DEVICES DEPLOYED



SECURITY ISSUES

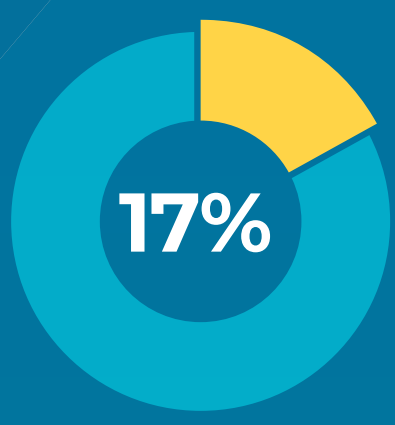




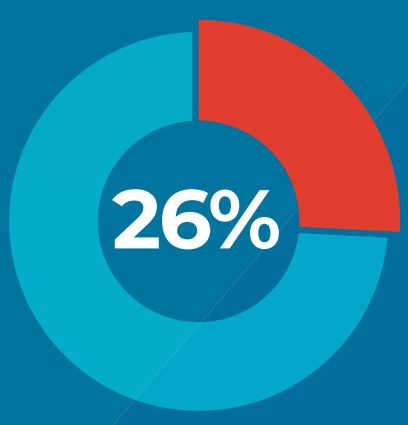
Patient Monitors

Patient Monitors often include cameras with default passwords, surveillance systems with unencrypted traffic, and recording systems accessible from the Internet. These devices contribute to Patient Monitors exhibiting the second leading security issues across all medical devices.

DEVICES DEPLOYED



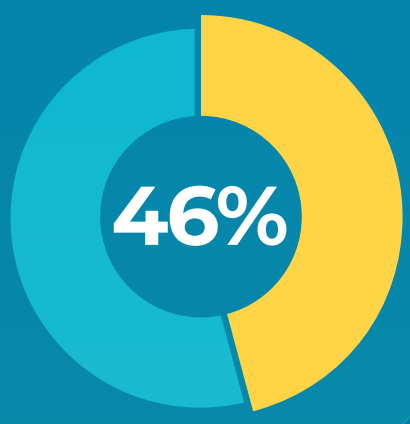
SECURITY ISSUES



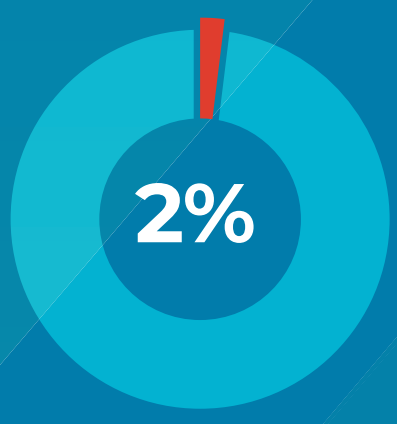
Infusion Pumps

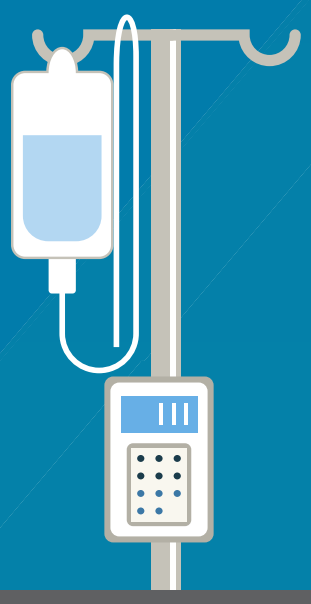
Despite being the most widely deployed connected device, infusion pumps almost never communicate externally and exhibit the lowest security issues.

DEVICES DEPLOYED



SECURITY ISSUES





Zingbox

Secure the devices that expose you to the biggest risks. To learn how, visit zingbox.com/healthcare.