Symantec™ Industry Focus:

Medical Device Security

MEDICAL DEVICE CYBERSECURITY

The cybersecurity posture of medical devices has increasingly become a concern to healthcare providers, device manufacturers, regulators, and patients. Due to their long useful life, unique care-critical use case, and strict regulatory oversight, these devices tend to have a low security maturity, significant vulnerabilities, and an overall high susceptibility to security threats. These include:

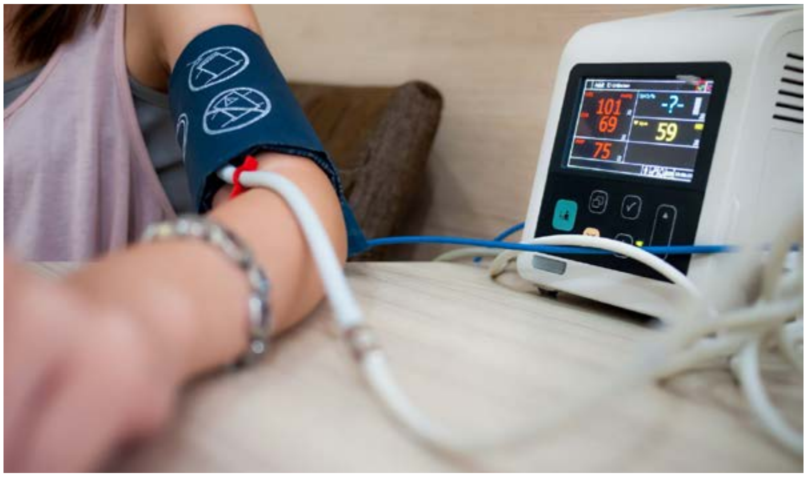
- A formal and highly regulated product release and distribution process that many believe prevents a nimble approach to cybersecurity;
- The use of commercial, off-the-shelf software components, such as operating systems, that inherit these components' respective vulnerabilities;
- Slow deployment of upgrades and patches and/or the issue of end-of-life software components that lead to an accumulation of security and privacy vulnerabilities; and
- Poorly protected devices and inadequately designed device networks that face a growing number of sophisticated and targeted attacks.

Medical devices now integrated with an increasingly digital healthcare infrastructure are exposed to the same security threats as any other IT component. Yet, defenses of these devices, as well as their integrated ecosystems, are far less mature.

In fact, medical devices represent a possible target for cybercriminals and could be exploited in a cyber-warfare, -terrorism, or vandalism attack. Healthcare organizations have also reported medical devices being shut down due to malware outbreaks — but not because they were targeted, rather because of their broad vulnerabilities that fit the malware's target profile. The possible consequences resulting from a medical device security incident can be severe and complex, with broad implications for patient health, care delivery, hospital revenue, manufacturer reputation, law suits and fines, and decision-making by patients about treatment options.

Increasing concerns are leading to mounting pressure to address these availability, integrity, and confidentiality challenges through a combined approach of technical, regulatory, and process measures. To address these issues, stakeholders must take a two-pronged approach that includes protecting the legacy devices used by hospitals and patients today and building security and information privacy measures into new devices and evolving mHealth care models.

KEY MILESTONES



2008: Pacemaker hack – Kevin Fu, UMass Amherst

2011: Insulin pump hack – Jerome Radcliffe, Black Hat Conference

2013: Discovery of a wide range of vulnerabilities across a variety of device types: Surgical and anesthesia devices, ventilators, infusion pumps, defibrillators, patient monitors, and laboratory equipment – Billy Rios, Security Researcher

2014: Multiple security alerts issued by ICS-CERT (Homeland Security / DHS), FBI, and FDA

2015: TrapX and Protiviti publish research demonstrating that medical devices are actively being exploited by cybercriminals as entry points for attacks on hospitals

2014 & 2016: FDA Cybersecurity Guidance for Premarket Submission and Postmarket Management is released

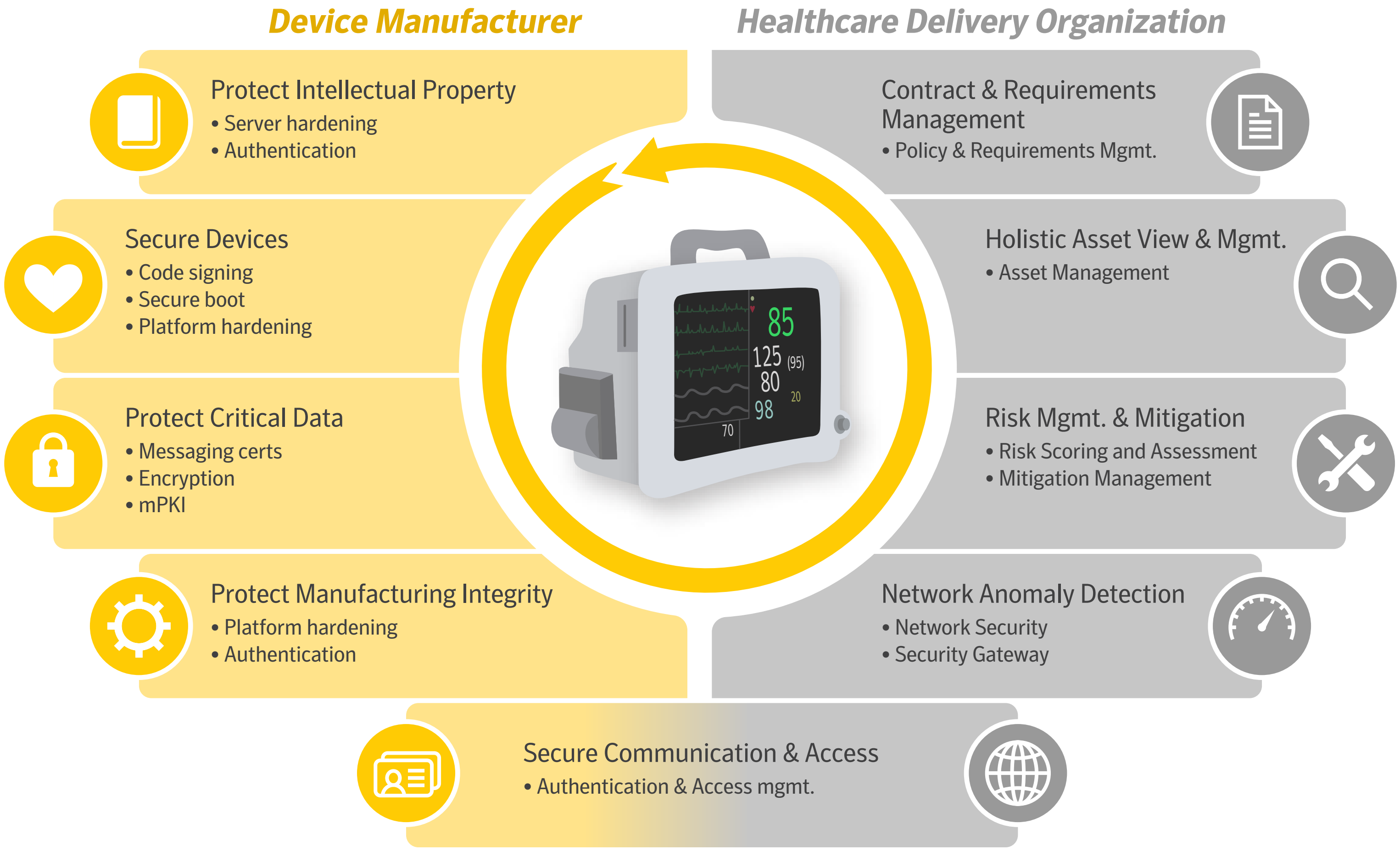
NEW PARADIGMS ARE EVOLVING

Cybersecurity Regulations: The increasing network integration of medical devices is leading to new patient safety risks. In October 2014, the FDA released industry guidance: *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, followed in January 2016 by *Postmarket Management of Cybersecurity in Medical Devices*. These documents assist with identifying issues related to cybersecurity that manufacturers should consider in the design and development (premarket) of devices, as well as the need for vulnerability sharing and management for devices circulating in the market (postmarket).

Risk Management: Recognizing the security risks introduced through medical device vulnerabilities and in order to comply with regional regulations (e.g. HIPAA for the U.S.), healthcare providers are including medical devices in their security risk analysis and management efforts. The ISO/IEC 80001 series of standards provides a framework specific to the medical device ecosystem by defining: Roles and responsibilities, activities, risk and lifecycle management, security capabilities, and guidance on specific topics (e.g. guidance for wireless networks).

Lifecycle Management and Procurement: Increasingly, healthcare organizations are taking active steps to protect their medical device ecosystems against cyber threats and risks. As part of their asset and risk assessment processes, they now articulate specific cybersecurity requirements and request disclosure of device cybersecurity properties as part of their purchasing process. Further, they segregate medical device networks and monitor security events on the network level.

MEDICAL DEVICE CYBERSECURITY — A SHARED RESPONSIBILITY



Device Manufacturer

Protect Intellectual Property
- Server hardening
- Authentication

Secure Devices
- Code signing
- Secure boot
- Platform hardening

Protect Critical Data
- Messaging certs
- Encryption
- mPKI

Protect Manufacturing Integrity
- Platform hardening
- Authentication

Healthcare Delivery Organization

Contract & Requirements Management
- Policy & Requirements Mgmt.

Holistic Asset View & Mgmt.
- Asset Management

Risk Mgmt. & Mitigation
- Risk Scoring and Assessment
- Mitigation Management

Network Anomaly Detection
- Network Security
- Security Gateway

Secure Communication & Access
- Authentication & Access mgmt.

RESOURCES

For more information, case studies, and white papers on medical device security, visit us at *www.symantec.com/healthcare* and *www.symantec.com/IoT*.

Confidence in a connected world.