Analyzing Risk in Connected Medical Devices

BY FORESCOUT RESEARCH LABS

Healthcare delivery organizations (HDOs) are dealing with increased risk due to skyrocketing numbers and types of interconnected devices, lack of network segmentation, unsupported OSes and insecure protocols. In addition, cybercriminals are discovering new ways to compromise devices and networks, as well as monetize patient data. It’s no wonder cyberattacks are on the rise.

Architecture of a Typical Healthcare Network

HDOs contain an average of 20,000 devices, including IT, IoMT, IoT and OT devices.

Potential Threats

LACK OF PROPER SEGMENTATION
- A broad range of IT, IoMT, IoT and OT devices are increasingly communicating on interconnected networks with minimal oversight
- A mix of personal and medical devices are often located on the same network segments
- Many medical devices use default credentials, making them the weak links in the network

UNSUPPORTED OSes
- Devices running vulnerable, unsupported OSes are often life-saving systems

USE OF INSECURE PROTOCOLS
- Insecure protocols and communications between public and private IP addresses exchange medical information in clear text

LEGACY SYSTEMS, IMPROPERLY SECURED EQUIPMENT & DEFAULT PASSWORDS
Many medical devices are legacy systems that cannot be patched due to availability or certification requirements

EXTERNAL THREATS
Cybercriminals or criminal organizations usually try to reap money from cyberattacks, either directly via ransomware and cryptomining or indirectly by selling stolen information or access to infected computers with botnets.

INTERNAL THREATS, VENDOR & CONTRACTOR ACCESS
HDOs aren’t just running emergency rooms and surgical clinics – they’re running remote access VPNs for vendor support and backend offices that require common (yet privileged) workstations. These open the network to the possibility of internal attacks, which may have a financial motivation or other goals such as sabotage

LACK OF PROPER SEGMENTATION
- A broad range of IT, IoMT, IoT and OT devices are increasingly communicating on interconnected networks with minimal oversight
- A mix of personal and medical devices are often located on the same network segments
- Many medical devices use default credentials, making them the weak links in the network

THE IMPORTANCE OF VISIBILITY
Cybersecurity for medical devices will be problematic for the next 20 years, and visibility is the key to improvement.

BEYOND VISIBILITY AND CONTROL: SECURITY AUTOMATION & ORCHESTRATION
Forrester defines visibility and analytics as the foundational prerequisites for Zero Trust and suggests that Zero Trust architecture can reduce an organization’s risk exposure by 37% while reducing security costs by 31%.

Reduction Risk: Key Takeaways

- 82% of U.S. hospitals reporting a significant security incident in 2018 or 2019
- 90% of VLANs with at least one healthcare device also have non-healthcare IoT devices
- 60% have IT devices with potentially vulnerable software or targeted malware
- 37% of device vulnerabilities are related to legacy systems
- 31% of risk exposure is related to legacy systems
- 25% of attacks are related to legacy systems

Get the full report at forescout.com/connected-medical-device-security-report

Don’t just see it. Secure it.™

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 10_20.