ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Fireside Chat:
Medical Device Security is a Joint Effort

Michael S. Brilling

Dartmouth-Hitchcock

Benjamin B. Stock

ordr

October 29, 2020

About the moderator

Kamecia Bruce | Acting Chief, Biomedical Engineering

Kamecia Bruce is currently Acting Chief Biomedical Engineer at the West Palm Beach VA Medical Center. She serves as Secretary of ACCE and graduated from Mississippi State University and the University of Rochester.

Logistics

- All attendees have their microphones muted during the presentation.
- Questions to the panelists must be submitted via the “Q&A” feature in Zoom at any time.
- If there is any urgent issue, please use the “chat” feature to communicate with the panelists.
- Please remember to complete the webinar evaluation after attending. A link will be provided at the end.

About the speaker

Dartmouth-Hitchcock

Michael S. Brilling

As a Mechanical Engineer, Michael started out working on large datacenter thermal efficiency. He spent several years in finance UNIX system administration and security. Since he's worked in healthcare, he's worked as a BMET, Clinical Engineer, and now as a manager.

About the speaker

ōrdr

Benjamin Stock is the Director of Healthcare Product Management at Ordr. Previously, Ben worked as the Director of Clinical Equipment Systems and Project Support at SSM Health St. Louis, MO. With more than 15 years of experience in healthcare technology management, his wealth of knowledge in the Clinical Engineering space allows him to be a wonderful advocate for Ordr healthcare customers. Ben is also a Certified Biomedical Equipment Technician (CBET).

Benjamin Stock

currently serves as Director of Healthcare Product Management at ORDR Inc.

Session Description

IoT and medical devices are revolutionizing patient care. However, these Internet of Medical Things (IoMT) are slow to adopt security practices and can be a challenge to secure. Despite clinical engineering, cybersecurity, and networking teams sharing the same objectives, in many organizations they are siloed. When it comes to developing a IoMT security strategy it's a team sport.

Join Michael Brilling, Manager, Clinical Engineering at Dartmouth-Hitchcock Health and Ben Stock, Director of Healthcare Product Development at Ordr in a fireside chat on how to drive cross functional collaboration to protect IoMT Devices.

The Healthcare Challenge: IoMT, OT and IoT

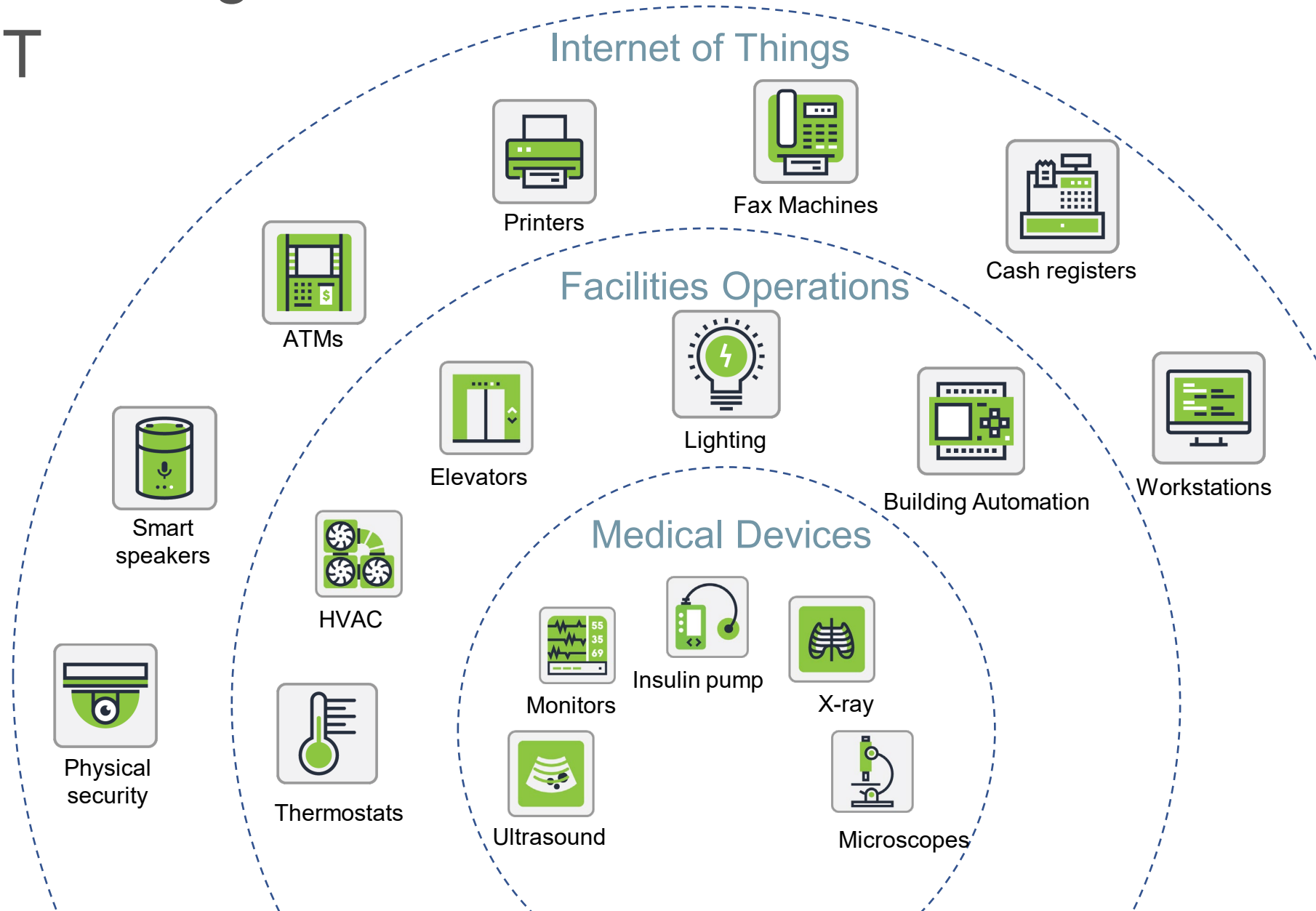
20,000 medical device manufacturers, resellers, and distributors

17 devices per hospital bed on average.

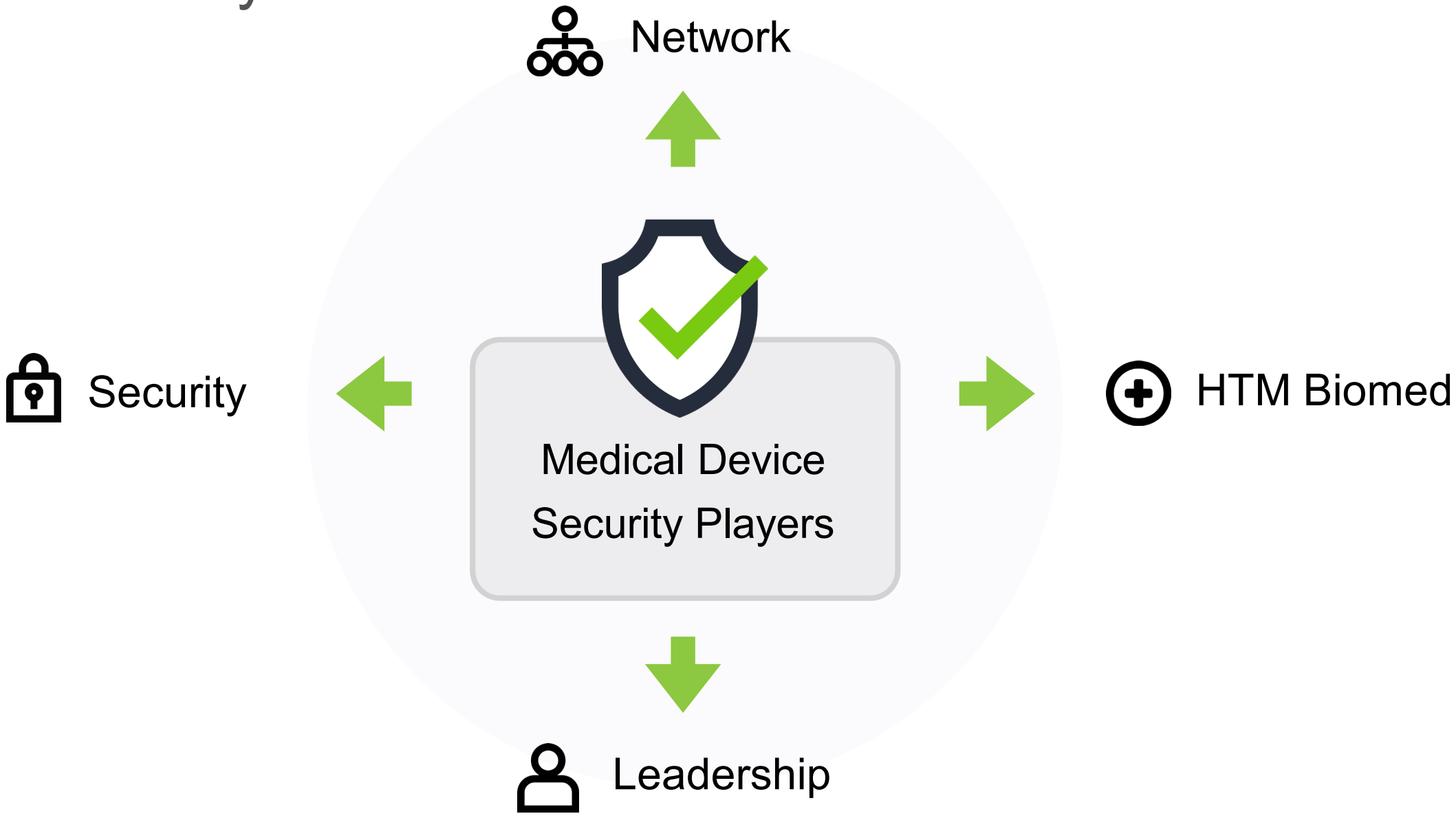
Thousands of unique legacy devices with old operating systems

Limited ability to patch, monitor and respond

Traditional cybersecurity capabilities are hard to apply



Know the Players



Teammate Challenges

Leadership

- Ensure all connected devices across the organization are secure
- Support finance procurement decisions with device utilization details

Security/IT

- Identify and secure all types of unmanaged IoT/IoMT devices
- Understand how each type of unmanaged device communicates on the network
- Build security policies to protect many types of vulnerable, unmanaged devices

Biomed

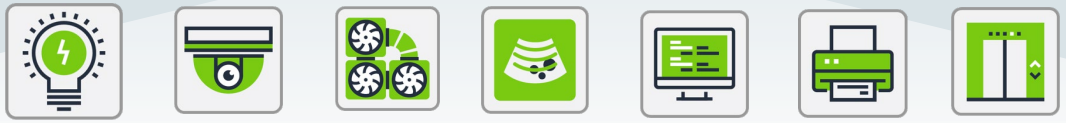
- Maintain a current list of all medical IoT devices (managed and unmanaged)
- Keep track of which medical devices have vulnerabilities or recalls
- Gain an understanding of how medical IoT devices are utilized

Introducing Ordr

ordr

SCE

AI-powered IoT security Platform for visibility and security of all unmanaged devices

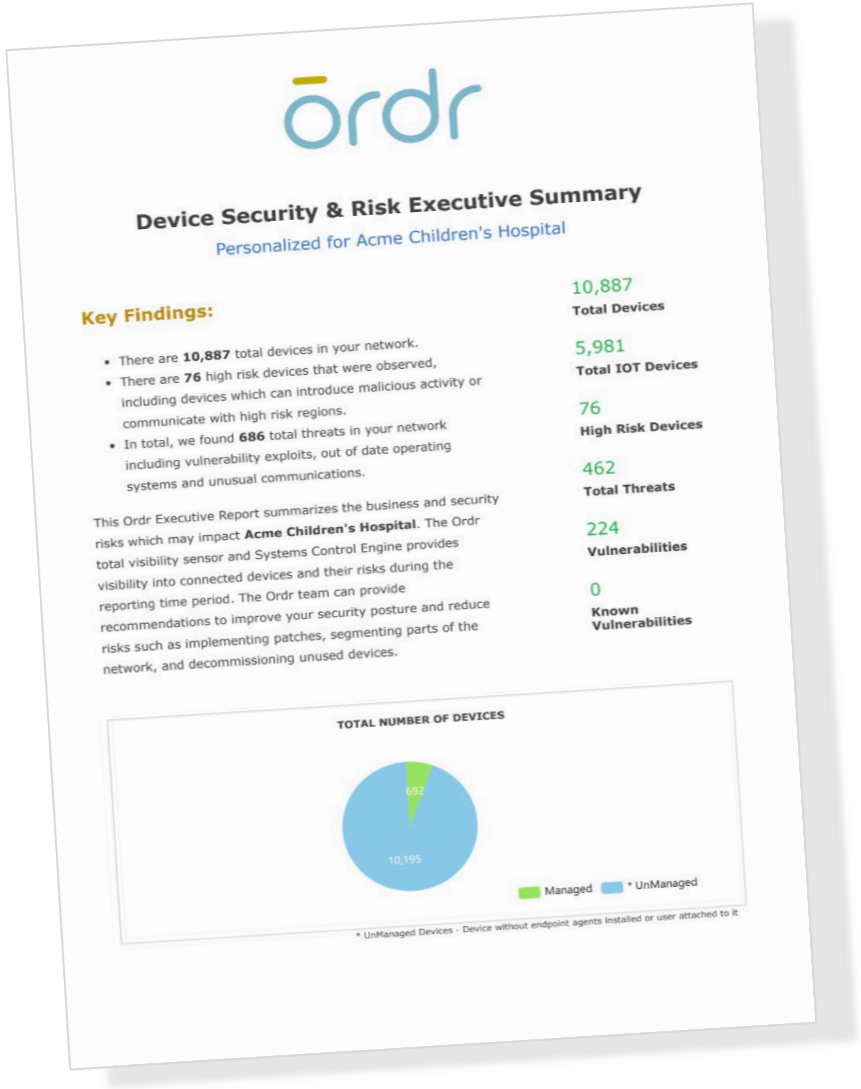


IoT, IoMT, OT devices

What devices are connected in my network?	What exactly are these devices doing?	How do I secure devices at scale?
Discover all devices • Agentless, zero touch deployment • Classify by make, model, serial number, location, O/S • Vulnerabilities, exploits, FDA recalls • Weak ciphers/certificates	**Profile behavior and risks** • Baseline communications • Visualize via VLAN and network arch • Anomalous and malicious behavior • Understand utilization of devices, who logged in and accessed device	**Automate action** • Proactive segmentation and enforcement on NAC, FW, switches • Trigger workflows for CMMS, CMDB • Incident response segmentation for vulnerable devices

Existing Network and Security Ecosystem

Ordr IoT Discovery Platform



ordr

Device Security & Risk Executive Summary

Personalized for Acme Children's Hospital

Key Findings:

- There are **10,887** total devices in your network.
- There are **76** high risk devices that were observed, including devices which can introduce malicious activity or communicate with high risk regions.
- In total, we found **686** total threats in your network including vulnerability exploits, out of date operating systems and unusual communications.

This Ordr Executive Report summarizes the business and security risks which may impact **Acme Children's Hospital**. The Ordr total visibility sensor and Systems Control Engine provides visibility into connected devices and their risks during the reporting time period. The Ordr team can provide recommendations to improve your security posture and reduce risks such as implementing patches, segmenting parts of the network, and decommissioning unused devices.

10,887 **Total Devices**

5,981 **Total IOT Devices**

76 **High Risk Devices**

462 **Total Threats**

224 **Vulnerabilities**

0 **Known Vulnerabilities**

TOTAL NUMBER OF DEVICES

692

10,195

Managed * UnManaged

* UnManaged Devices - Device without endpoint agents installed or user attached to it

Sign up at **www.ordr.net/sensor**

How It Works:

1. Receive our free, lightweight, zero touch provisioning sensor
2. Deploy it in your network
3. Gain visibility into what devices are connected, what they are doing, and the risks they bring in minutes
4. Get an IoT Discovery Report at the conclusion of the program


Questions

ACCE Membership

Not a member yet? Apply Now!

https://accenet.org/Membership/Pages/ApplicationForms.aspx

Benefits	Discounts
Bi-monthly ACCE newsletter, timely updates and articles	AAMI, HIMSS, IFMBE conference registration
Complimentary ACCE receptions	JCE Journal
Volunteer opportunities	ACCE educational content
Complimentary educational webinar	Free access to IFMBE/Springer publications

Already a member? Invite a colleague to join.

Thank You

Please complete the online evaluation/attendance form at
www.surveymonkey.com/r/ACCE_10-29-20

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING