MEDIGATE

MEDICAL DEVICE SECURITY REQUIRES CLINICAL EXPERTISE

1

WHY IS IT MORE CHALLENGING TO SECURE MEDICAL DEVICES?

Firewall
Reliance on generic identifiers like IP addresses results in non-granular, generic, and inefficient rules.

NAC
Devices that were not designed to be network-managed are difficult to identify properly and lead to subpar access policies.

Endpoint Security
Proprietary and legacy operating system, as well as manufacturer warranties, makes deploying EPS unfeasible.

2

WHAT DOES CLINICAL EXPERTISE MEAN FOR SECURITY?

Communication Protocols
Understanding what a device was designed to communicate and for what purposes.

Intended Workflows
Knowing, exactly not guessing, what the device can an cannot communicate with, and under what conditions.

Unique Device Signatures
Recognizing what trace it will and will not leave on the network.

3

HOW CLINICAL EXPERTISE POWERS IoT & IoMT SECURITY?

Visibility
Fingerprinting connected devices requires a deep understanding of proprietary device communication protocols and clinical workflows across vendors and models.

Detection
Clinical domain expertise detects activity that is out of clinical scope of its intended workflow, generates non-generic alerts and minimizes false positives.

Prevention
Successful micro-segmentation, security policies, and VLAN assignments rely on accurate device identification with clinical context.

SOLVING IoT & IoMT DEVICE SECURITY CHALLENGES FOR HEALTHCARE

IDENTIFICATION DETECTION PROTECTION RISK MGMT RISK MITIGATION ROI

NETWORK PRODUCTS GUIDE IT World Awards 2019 GOLD

MOST INNOVATIVE COMPANIES FAST COMPANY

constellation ShortList™

BIG 50 2016 STARTUP 50

Contact us at info@medigate.io or visit www.medigate.io to learn how we do it.