LOCH TECHNOLOGIES

Heathcare Solutions

Zero Trust Security for IoMT Wireless Edge

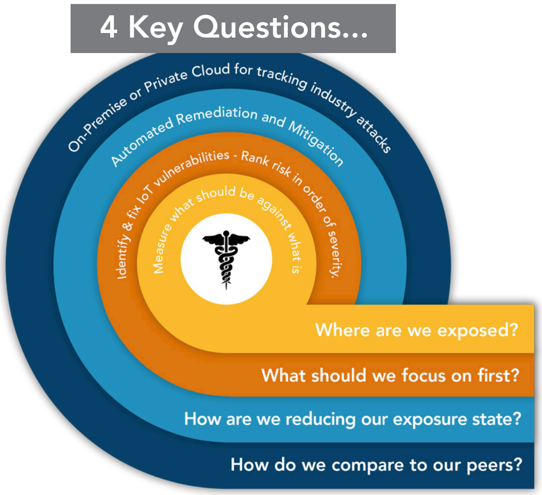
Protect your Healthcare Organization from Wireless and IoT Risks

The use of connected IoMT devices operating across either cellular or broad spectrum radio frequencies means faster digital transformation for healthcare delivery organization (HDOs), but it comes with risk. According to Deloitte, wirelessly connected devices are expected to have spend of around $50B by 2022.

IoMT has created the world's largest attack surface, the scope of which is only broadening with exponential growth in deployment of 5G/LTE. Today's networks and organizations were never built to handle this extraordinary volume, velocity, and hyperconnectivity of IoMT technologies in the modern hospital. This reality has created critical security gaps for healthcare organizations hoping to benefit from the promise of IoMT products, applications, and services.

The LOCH Wireless Machine Vision™ platform provides next-generation wireless AI driven threat intelligence across 4G and 5G deployments, broad-spectrum wireless IoT, Citizens Broadband Radio Service (CBRS) as well as 802.11/Bluetooth WiFi environments by providing customers with full IoT discovery, asset classification, risk analysis and actionable remediation capabilities based on a zero trust framework.

4 Key Questions...



On-Premise or Private Cloud for tracking industry attacks

Automated Remediation and Mitigation

Identify & fix IoT vulnerabilities - Rank risk in order of severity.

Measure what should be against what is

Where are we exposed?

What should we focus on first?

How are we reducing our exposure state?

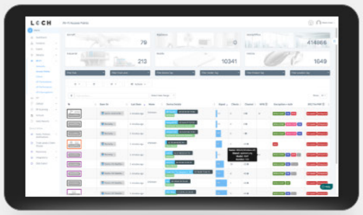
How do we compare to our peers?

IoT Threats Impacting Healthcare

- Inadequate Network Segmentation
- Outdated OS or Lack of Security Patches
- Device Spoofing or Hijacking
- Malware Injection
- Weak or Lack of Encryption

Solution Benefits

DETECT

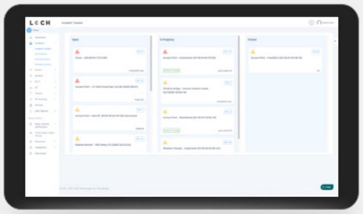


- Detect, identify & classify all broad spectrum RF emitting devices in range
- Device and network pairing communication map analysis and correlation
- Risk assessment threat ranking for Zero Trust network access control
- Mobile App for hunting rogues even if mobile

TRACK

- Wireless deep packet inspection
- Behavioral baselining, analysis and anomaly detection/alerts
- DVR-like capabilities for forensics, including geo-positioning
- Carrier integration with cellular devices for anomaly detection, fraud/theft and cost management

REMEDIATE



- List & map devices on dashboard or directly into SIEMs.
- Interact with MDM & EMM assets for correlation & feedback on exceptions
- Rectify network segmentation via interactions with SOAR, FW and/or NAC systems
- Automate response & closure via collaboration with ITSM/ITSL & CMDBs

Rogue Cell Tower Detection - Prevent authorized devices from connecting to unauthorised cell towers

Detect and Prevent Evil Twin Attacks - Prevent authorized devices from connecting to unauthorised Wi-Fi Access Points

Roaming - prevent increase in data usage and excessive billing. Monitor potential data exfiltration against traffic base line to flag malware and bots.

Prevent Device Threats - Malware, Firmware Hacks, Sensor IoT Compromises, Man In the Middle Attacks, Device Tampering

Key Differentiators

- **Single pane of glass** to manage ALL wireless threats across cellular 3G/4G/5G, broad-spectrum wireless, CBRS and 802.11/Bluetooth Wi-Fi devices
- **Early Warning System** - detecting threats before they hit the wired network
- **Edge IoT Vulnerability Scanning** to detect open ports & services to identify exposed threats before they are abused
- **Monitor Enforce Zero-**Trust Policies and "No Phone" Zones
- **Deployable** in air-gapped environments also
- **API driven integration** with wide ecosystem for automated remediation and collaboration

www.loch.io

LOCH TECHNOLOGIES

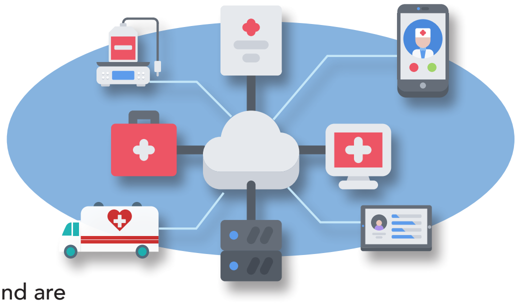
Invisible Threats. Visible Protection

Detect, Track and Secure IoMT devices within your environment

Unique RF in Healthcare Environments

- HL7 Interface from Monitoring Device
- Wireless Medical Telemetry Service (WMTS) – 608-614, 1395-1400, 1427 - 1432 MHz
- Medical Device Radio Communications Service (MedRadio) - 400, 2360 - 2400 MHz

IoMT wireless has created a new invisible attack surface



LOCH Security for Healthcare IoMT

- **Wireless IoMT Deployments:** In environments where Wireless/RF is used for connectivity, LOCH is the single truth for all device inventory. If they are out there and are transmitting, we will know and can physically pinpoint them.
- **IoMT Security:** Cybersecurity tools that manage such devices are based on network side solutions that use deep packet inspection and protocol dissection of flows from the subnets/VLANs. LOCH's auto discovery will find devices that were missed due to incorrect subnet/VLAN configuration or lack of deployment.
- **IoMT Device Scanning:** LOCH solutions will include a lightweight 'outside-in', continuous edge vulnerability management solution to provide device details and scan them for threats and misconfigurations.
- **4G/5G Security:** In addition to traffic monitoring against established baseline for anomalies LOCH can sense the presence of adjacent RF channels to thwart man-in-the-middle hijack attempts.
- **LTE Connectivity:** LOCH delivers the ability to monitor traffic from SIMs to alert on excessive use and changes in Device/SIM association.

Security Posture and Operational Efficiency for IoMT Devices

Patient Monitoring - critical for tracking and notifying on patient stats. Detect and eliminate RF interference.

Syringe Pumps – critical for patient care. Ensure proper network segmentation and block unauthorized access.

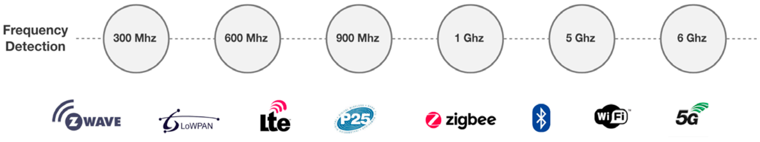
Infusion Pumps - critical for patient care. Ensure proper network segmentation and block unauthorized access.

WiFi Connected Beds – cause major interference with other medical devices due to excessive probing and constant reconnects.

Ultrasound – mobile and connected to WiFi. Ensure proper network segmentation and scan for OS vulnerabilities.

Analog Pagers – PHI information shared via unencrypted analog pagers violates HIPAA compliance.

Medical Laptops – storing and tracking patient health information. Scan for vulnerabilities.



LOCH Core Competencies in Healthcare

- Software defined radios to detect broad spectrum RF
- Comprehensive classification of all assets in the environment and continuous Intrusion Detection
- Wireless Security Threat Research for rapid anomaly detection
- Decoding of IoMT operating systems and protocols
- Zero-Trust Policy Enforcement
- Rogue Cellular Tower and Stingray Detection
- API integrations for threat mitigation & remediation

info@loch.io | 1-888-725-9434 | www.loch.io

| LOCH Technologies, Inc. 1285 66th Street, Emeryville, CA 94608